Table of Contents

HIPAA at Boston University ........................................................................................................................... 1

Privacy and Security .................................................................................................................................. 1

Policy Responsibility .................................................................................................................................. 1

1. HIPAA Basics .............................................................................................................................................. 2

1.1 HIPAA Covered Components .............................................................................................................. 2

1.2 Key Roles ............................................................................................................................................. 2

1.3 What is PHI? ........................................................................................................................................ 3

1.4 De-Identified PHI ................................................................................................................................. 4

1.5 The Covered Component’s Designated Record Set ............................................................................ 5

1.6 The Covered Component’s HIPAA Workforce .................................................................................... 5

1.7 Access to PHI ....................................................................................................................................... 6

1.8 HIPAA Training .................................................................................................................................... 6

2. Individual Responsibilities for Safeguarding PHI ....................................................................................... 8

2.1 Safeguarding Paper and Other Tangible PHI ....................................................................................... 8

2.2 Safeguarding Verbal PHI ..................................................................................................................... 8

2.3 Safeguarding Electronic PHI ................................................................................................................ 9

3. Using PHI in Treatment, for Payment and for Health Care Operations; Business Associates ........ 11

3.1 Overview ........................................................................................................................................... 11

3.2 Minimum Necessary Rule .................................................................................................................. 11

3.3 Special Rules for PHI in Limited Data Sets ........................................................................................ 11

3.4 Patient Authorization Not Needed for Treatment Purposes ............................................................ 12

3.5 Using PHI for Payment Purposes ...................................................................................................... 13

3.6 Using PHI for Health Care Operations Purposes ............................................................................... 13

3.7 Routine Disclosures to an Individual’s Family and Friends ............................................................... 14

3.8 Sharing PHI with the Patient’s Other Providers and Health Plans .................................................... 15

3.9 Disclosing PHI to Business Associates ............................................................................................... 16

4. Uses Required or Permitted by Law; Prohibited Uses of PHI; ............................................................... 19

4.1 Required by Law................................................................................................................................ 19

4.2 Prohibited Uses of PHI: Marketing; Sale; non-BU Purposes ............................................................... 20
4.3 Fundraising and Promotion ................................................................. 21

5. Situations in which Authorizations are Necessary ................................ 23

5.1 General Rules on Authorization .......................................................... 23
5.2 Parents, Guardians and Minors ............................................................. 25
5.3 Legally Authorized Representative of an Adult Patient ...................... 26
5.4 After a Patient’s Death ........................................................................ 27
5.5 Research: Authorizations and Waivers .............................................. 28
5.6 Students and Observers ........................................................................ 29
5.7 Using PHI in Publishing ..................................................................... 30

6. Individuals’ rights under HIPAA ......................................................... 31

6.1 Right to Notice of Privacy Practices .................................................. 31
6.2 Right to Access and Copy Own Health Record ................................. 31
6.3 Right to Request Amendment ............................................................ 34
6.4 Right to an Accounting of Disclosures ............................................. 36
6.5 Right to Request Restriction .............................................................. 38
6.6 Right to Request Confidential and Alternate Modes of Communications 39
6.7 Right to Complain ............................................................................... 40

7. Breaches ............................................................................................. 41

7.1 Obligation to Report Potential Breaches ............................................ 41
7.2 No Retaliation .................................................................................... 41
7.3 Investigation and Remedial Action for Reports of Potential Breaches: 41
7.4 Breach Notifications .......................................................................... 42
7.5 Enforcement and Sanctions ............................................................... 42

8. HIPAA Security Program ..................................................................... 43

8.1 Identify ............................................................................................. 43
8.1.1 PHI Inventory ................................................................................ 44
8.1.2 Security Risk Assessments ......................................................... 44
8.1.3 Periodic Technical and Non-Technical Security Reviews .......... 45
8.2 Protect ............................................................................................... 45
8.2.1 Individual Responsibilities .......................................................... 45
8.2.2 Administrative Controls: Training, Access Management .......... 46
<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>8.2.3 Technical Controls</td>
<td>46</td>
</tr>
<tr>
<td>8.2.4 Physical Controls</td>
<td>47</td>
</tr>
<tr>
<td>8.4 Respond</td>
<td>49</td>
</tr>
<tr>
<td>8.5 Recover: Contingency Planning; Emergency Mode Operations; Recovery</td>
<td>49</td>
</tr>
<tr>
<td>9. Documentation and Retention</td>
<td>52</td>
</tr>
<tr>
<td>10. Exceptions</td>
<td>53</td>
</tr>
</tbody>
</table>

Appendix A
HIPAA at Boston University

These policies are intended to guide the health care provider units of Boston University that are covered by the Health Insurance Portability and Accessibility Act (“HIPAA”) in complying with HIPAA’s requirements. Those units are referred to as Covered Components. Separate policies apply to the BU Health Plans, which are Covered Entities.

The Covered Components and their Workforces are required by HIPAA to ensure the privacy and security of all protected health information (“PHI”) that they create, receive, maintain, or transmit. PHI subject to HIPAA may exist in any form including paper, electronic, or verbal. They also observe the rights of individuals regarding their PHI as mandated by HIPAA.

These policies supersede and replace all prior policies concerning HIPAA at BU, and they supplement other policies of the University. For example, under the University’s Data Classification policy, individually identifiable health information that is subject to HIPAA (“PHI”) is categorized as Restricted Use information, meaning that it requires the greatest protection of all data types at the University and breaches of this data are potentially reportable to state and/or federal authorities.

Privacy and Security

The Privacy Rule describes who can access, use, and disclose PHI, and for what purposes. The Privacy Rule also describes how Covered Components must assist Individuals with exercising their rights under HIPAA to access and control the use of his or her PHI.

The Security Rule describes how to protect electronic PHI (“ePHI”) when using, storing, or transmitting it to minimize the chance that it will fall into the wrong hands. Links are provided to pertinent BU Information Security policies.

Policy Responsibility

These HIPAA Privacy and Security Policies apply to all Boston University designated Covered Components. Those primarily responsible for implementation of these policies are:

- BU’s HIPAA Privacy Officer is responsible for development and implementation of BU-wide HIPAA privacy policies.
- BU’s HIPAA Security Officer is responsible for development and implementation of BU-wide HIPAA security policies to protect ePHI.
- Each Covered Component has a HIPAA Contact, responsible for implementation of procedures to implement these policies in their units, documenting HIPAA compliance, and the other duties listed in Appendix A.
- Every member of each Covered Component Workforce is responsible for understanding and complying with these policies and the Covered Component’s procedures.

Defined terms used in these policies are capitalized. The definitions of those terms are found in Policy 11, Definitions.
1. HIPAA Basics

1.1 HIPAA Covered Components

**BU Covered Components**

BU is a hybrid entity under HIPAA, meaning some of its operations are covered by HIPAA but many are not, and HIPAA allows BU to designate which of its components are HIPAA Covered Components. The following are the BU health care provider Covered Components:

1. Boston University Rehabilitation Services (including the BU Physical Therapy Center and BU Center for Neurorehabilitation),
2. Sargent Choice Nutrition Center,
3. Henry M. Goldman School of Dental Medicine Patient Treatment Centers, including the BU Dental Health Center,
4. The Albert and Jessie Danielsen Institute

Boston University Student Health Services fits the statutory definition of a Covered Component, but its records are either Education Records or Treatment Records under the Family Educational Rights and Privacy Act, 20 U.S.C. Section 1232g. As a result, Student Health Services is not subject to either the HIPAA Privacy Rule or the HIPAA Security Rule and is not subject to these policies.

**Support Units**

Each of the Covered Components receives services from a number of BU units that are not Covered Components. These are referred to as Support Units. BU Support Unit employees who use or disclose PHI in the course of providing services to any Covered Component have the same responsibilities to protect PHI as members of the Workforce of the Covered Component.

BU has identified the following units as Support Units whose services to Covered Components commonly use or disclose the Covered Component’s PHI:

- Information Services & Technology, including Boston University Medical Campus Information Technology
- Financial Affairs, including Internal Audit and Advisory Services, Risk Management, and Accounts Payable
- Office of the General Counsel

Note: BU maintains many types of sensitive information not subject to HIPAA, such as student records whose confidentiality is governed by FERPA; patient records in units that do not conduct electronic transactions that make them subject to HIPAA but remain subject to state law; human resources records governed by federal and state law, and certain human subjects research data protected by federal and state laws. BU takes seriously its obligations under each of these laws and protects those records accordingly.

1.2 Key Roles

The HIPAA Privacy and Security Officers are your primary resources for HIPAA Compliance. You may reach them at the following e mail address: hipaa@bu.edu. Use that address to ask questions or to
The BU HIPAA Security Officer is responsible for the development and implementation of policies to ensure compliance with HIPAA’s Security Standards.

The BU HIPAA Privacy Officer is responsible for the development and implementation of policies to ensure compliance with HIPAA’s Privacy Standards.

Covered Component HIPAA Contact:
Each Covered Component must designate one person to serve as the Covered Component HIPAA Contact, responsible for implementing these HIPAA policies in that Covered Component.

The BU HIPAA Privacy Officer and BU HIPAA Security Officer work closely with each Covered Component’s HIPAA Contact on implementation of HIPAA compliance in their units and serve as key resources.

The persons serving in these key roles are listed in Appendix A.

1.3 What is PHI?
Protected Health Information (PHI) is any indvidually identifiable health information that can be linked to a particular person. It includes all information that was received, created, used, or disclosed in the course of providing a health care service such as diagnosis or treatment. This information relates to:

- The individual’s past, present or future physical or mental health or condition;
- The provision of health care to the individual; or,
- The past, present, or future payment for the provision of health care to the individual.

What is not PHI?
Health information that does not identify an individual or that cannot be used to identify an individual is not PHI, but great rigor is required to confirm that no identifier is present in the dataset. For example, a data set of vital signs by themselves do not constitute PHI. However, if the vital signs data set includes medical record numbers, then the data set has not been successfully de-identified and must be protected as PHI.

Some types of health information are not subject to HIPAA, even if they clearly identify the individual:

- Research data that identifies an individual in research performed by an entity that is not subject to HIPAA,
- Information in treatment and education records covered by FERPA,
- Information in treatment records retained by BU health care provider units that are not designated as Covered Components,
- Health information in medical records about a person who has been deceased for more than 50 years,
- Information in BU’s Human Resources employment records, and
- De-identified data, as described in Section 1.4: De-Identified PHI, below.
The types of information listed above are not subject to this Policy, but must be protected as set forth in the University’s Data Protection Standards.

1.4 De-Identified PHI

If PHI is de-identified in the manner described below, the resulting data is no longer PHI and its use and disclosure will not be subject to HIPAA. Thus, no individual Authorization is needed to use the de-identified data.

There are two methods for de-identifying.

Removal of Identifiers Method
All of the following identifiers of the individual and of relatives, employers, or household members of the individual, are removed:

(i) Names;
(ii) All geographic subdivisions smaller than a State, including street address, city, county, precinct, zip code, and their equivalent geocodes, except for the initial three digits of a zip code if, according to the current publicly available data from the Bureau of the Census:
   (1) The geographic unit formed by combining all zip codes with the same three initial digits contains more than 20,000 people; and
   (2) The initial three digits of a zip code for all such geographic units containing 20,000 or fewer people is changed to 000;
(iii) All elements of dates (except year) for dates directly related to an individual, including birth date, admission date, discharge date, date of death; and all ages over 89 and all elements of dates (including year) indicative of such age, except that such ages and elements may be aggregated into a single category of age 90 or older;
(iv) Telephone numbers;
(v) Fax numbers;
(vi) Electronic mail addresses;
(vii) Social security numbers;
(viii) Medical record numbers;
(ix) Health plan beneficiary numbers;
(x) Account numbers;
(xi) Certificate/license numbers;
(xii) Vehicle identifiers and serial numbers, including license plate numbers;
(xiii) Device identifiers and serial numbers;
(xiv) Web Universal Resource Locators (URLs);
(xv) Internet Protocol (IP) address numbers;
(xvi) Biometric identifiers, including finger and voice prints;
(xvii) Full face photographic images and any comparable images; and
(xviii) Any other unique identifying number, characteristic, or code.

On rare occasions, even when PHI is de-identified, the individual can be identified. Typically, that occurs when the patient’s condition and/or circumstances are very rare and/or may have been publicized. Thus, even when the 18 identifiers are removed, the Covered Component needs to confirm there is no reasonable basis to believe that the information could be used to identify an individual.
The BU HIPAA Privacy and Security Officers are available to confirm the information has been adequately de-identified, or to assist with obtaining the data in another form.

**Expert Opinion Method**

If a Workforce member believes the data s/he wishes to use cannot be linked to an individual, but it does not meet the criteria for “de-identified” (for example, dates of treatment are included), the Workforce member should contact the BU HIPAA Privacy Officer for assistance in obtaining an expert opinion that the risk is very small that information could be connected to an individual. There are specific requirements to be followed under HIPAA in using this method, and the HIPAA Privacy Officer can ensure the regulations are followed.

**Re-Identifying De-Identified PHI**

The Covered Component may, at its discretion, decode or translate de-identified PHI in order to re-identify the information with respect to specific individuals. The following requirements must be met:

- The re-identification process must be performed in a secure manner;
- The code, algorithm, table or other tool for re-identification may not be disclosed to any third-party or used for any purpose other than re-identification by the Covered Component; and
- The re-identification process utilized must be incapable of being translated or decoded by a third-party so as to identify the patient (e.g., the code cannot be a derivative of the patient’s name).

**1.5 The Covered Component’s Designated Record Set**

The Designated Record Set includes the Individual’s medical records that are used, in whole or in part, by the Covered Component to make decisions about an Individual. Typically included are the provider’s assessment and care of the Individual including diagnoses, diagnostic studies and tests, treatment, outcome, referrals, and disposition. The Designated Record Set also includes all billing records.

The Designated Record Set is important in fulfilling Individuals’ rights under HIPAA. For example, when an Individual requests access to or a copy of his/her record, it is the Designated Record Set that is provided.

The Covered Component HIPAA Contact is responsible, with guidance from the BU HIPAA Privacy Officer, for determining and recording the Covered Component’s Designated Record Set. Various portions of the Designated Record Set may be maintained in multiple locations within the Covered Component, and may include paper PHI, electronic PHI and other tangible PHI such as X rays, microfiche, photographs and audio recordings.

**1.6 The Covered Component’s HIPAA Workforce**

The HIPAA Workforce consists of all faculty, employees, volunteers, health care providers, trainees (students participating in treatment), and other persons whose work is under the control of the HIPAA Covered Component, regardless of whether they are paid directly by a HIPAA Covered Component, whose work requires accessing, using, disclosing or creating PHI of that Covered Component.

Note: Students who do not participate in providing care and persons shadowing care providers are not members of the Workforce. See Section 5.6: Disclosures of PHI to Students and Observers, below.
Designation of Covered Component Workforce
The Covered Component’s HIPAA Contact is responsible, with guidance from the BU HIPAA Privacy Officer, for designating and documenting who is in the Covered Component’s HIPAA Workforce, and for updating the designation continually as needed.

Designation of the Covered Component Workforce is to be recorded by each Covered Component in the BU HIPAA SharePoint site, including each person’s name, title, level of access to PHI, assigned training and completion of training.

1.7 Access to PHI

Levels of Access
The Covered Component HIPAA Contact is responsible for determining the level of access to PHI to be provided to each Workforce Member, and for documenting and monitoring that access level, with guidance from the BU HIPAA Privacy Officer and HIPAA Security Officer. Access must be role based; in other words, the level of access granted to each individual depends upon the type of PHI required by the Workforce member to carry out his/her duties. Health care providers should have unrestricted access to their patient records.

Termination of Access
The Covered Component HIPAA Contact is also responsible for ensuring access to PHI is terminated when a person is no longer a member of the Workforce due to termination of employment, reassignment to a position at BU outside the Covered Component, change in duties affecting need for access to PHI, retirement, extended leave (beyond 2 months) or any other reason. In addition, the HIPAA Contact needs to ensure the departing Workforce Member has not retained any BU PHI or other confidential BU data on devices or in any other form.

This includes immediately:
- terminating access to the premises by requiring the return of keys and badges,
- terminating electronic access to applications, systems or facilities, and
- ensuring departing Workforce members leave at BU any tangible PHI and remove any ePHI they may have received while in the Workforce from any device that they are not leaving with the Covered Component upon exiting.

Documentation and Local Auditing
Covered Component HIPAA Contacts are responsible for creating procedures that define how access to ePHI is authorized, maintained, and revoked. Typically, this will consist of a matrix listing all Workforce members and their access rights.

See Policy 8, below, on access management.

1.8 HIPAA Training
All members of the Workforce of each BU Covered Component and Support Unit employees who support the Covered Components and who may have access to PHI are required to complete Boston University HIPAA training, as specified by the BU HIPAA Privacy Officer and the BU HIPAA Security Officer. This training will explain the privacy and security provisions of HIPAA as well as providing an
overview of BU’s HIPAA Privacy and Security policies. A new member of a Covered Component’s Workforce or of a Support Unit shall complete training before having access to any PHI and all will complete refresher HIPAA training annually thereafter.

Responsibilities of Covered Components
The Covered Component HIPAA Contact must ensure training is completed as required by this Policy and must track and document the completion of training by each Workforce Member.
2. Individual Responsibilities for Safeguarding PHI

2.1 Safeguarding Paper and Other Tangible PHI
Anyone who uses or discloses PHI is responsible for taking appropriate precautions to prevent unauthorized physical access to it during the course of daily operations. For example:

- Do not remove paper or tangible PHI from a Covered Component unless approved by the HIPAA Contact;
- If you are allowed to remove PHI, do not leave it, or any file, box, briefcase or portable electronic device containing it, anywhere they can be easily stolen, such as cars;
- Avoid displaying or storing PHI in public spaces or in spaces that visitors must pass through to access other parts of the facility;
- Report any suspicious activity, including apparent physical maintenance to a Covered Component’s facility that seems inappropriate or unscheduled;
- Do not leave PHI on desks when not working on it. Safely store PHI even if you step away from your desk or work area just for a minute;
- Lock all PHI away at night in a cabinet or locked office;
- If a Covered Component facility is visible from the exterior, close window blinds to prevent outside disclosure;
- Never dispose of paper or other tangible PHI in the trash. Use a cross-cut shredder;
- Do not store a “shred box” under your desk. It’s too easy for cleaning staff to confuse it with trash and dispose of it in a non-secure manner;
- Off-site storage of paper records may be used, provided the storage company offers appropriately secure conditions and signs a Business Associate Agreement;
- Transmitting paper or other tangible PHI by US Mail or reliable delivery services such as UPS, FedEx and DHL is permissible, but use common sense in not overstuffing envelopes, and use appropriate boxes and envelopes to minimize the possibility of loss in transit;
- Transmitting paper PHI via facsimile is permissible. Please program frequently used numbers into the fax machine, and confirm you are faxing to the correct number.

2.2 Safeguarding Verbal PHI

Conversations
Do not discuss patients in a public area such as the waiting room, cafeteria, restaurant, street, elevator, stairwell or any place else. You may think you are masking the patient’s identify by not using a name or telling all of the details, but someone who overhears may recognize the person; in any event, such conversations reflect poorly on us and even if deidentified, are still inappropriate.

Waiting Room Configuration
Arrange the waiting areas in such a way as to minimize one patient overhearing conversations with another. Useful approaches include:

- Posting a sign to keep patients waiting in line back from reception conversation, or
- Ambient music or white noise to cover reception conversation.
PHI on the Telephone
Landlines and mobile phones are reasonably secure and may be used to communicate PHI.

- Callers should still use common sense precautions, such as ensuring no one in the vicinity can overhear what is said.
- Avoid use of a speaker phone if unauthorized persons could hear the conversation.
- When leaving a voice mail for an Individual, leave the minimum necessary information unless the patient has authorized you in writing to leave substantive messages. A minimum necessary voice mail would be something like, “This voice mail is for [patient name]. This is [your name] at the [Covered Component name]. Please return my call at 617-xxx-xxxx.”

2.3 Safeguarding Electronic PHI

1. Only use electronic devices that are approved for use by the Covered Component in its procedures.
2. Only store ePHI on devices approved by the Covered Component.
3. Only share ePHI using applications and storage locations approved by the Covered Component.
4. If a Covered Component’s procedures allow its Workforce Members to access ePHI from a personal device, those personal devices must meet the standards set in Policy 8, HIPAA Security Program, including encryption; password protection; anti-malware and other such measures described in Policy 8.
5. When sending ePHI via email:
   a. Ensure the recipient is authorized to have access to the ePHI;
   b. Use encryption such as:
      i. an approved email communication tool (DataMotion);
      ii. Encrypt the document or spreadsheet before sending. See Microsoft Support Article. If you choose to encrypt the document and send it via non-secure email, take care to avoid identifying the patient in the subject line or body of the email.
   c. If a patient requests use of non-secure email, follow Section 6.6: Right to Request Confidential and Alternate Modes of Communications that addresses non-secure email Requests.
6. Do not send PHI via text message:
   a. You may send de-identified patient information to co-workers in a text message, for example, “your 2:00 appoint called to cancel” or “can we meet at noon tomorrow to discuss our new patient with Parkinson’s?”
   b. If a patient requests use of text messaging, follow Section 6.6: Right to Request Confidential and Alternate Modes of Communications that addresses non-secure email/text requests.
7. Do not position monitors displaying ePHI where they can be viewed by the public.
8. Use PHI only with applications and systems approved by your HIPAA Contact.
9. Protect accounts, passwords, and workstations:
   a. Create and periodically change passwords that conform to best practices for selecting passwords even when not enforced by the system;
b. Immediately change your password and notify Information Security if there is reason to believe that a password has been improperly disclosed, accessed or used by an unauthorized person;

c. Do not share passwords related to any University system with any other person;

d. Do not use University passwords for any non-University accounts; and

e. Only use administrator accounts with privileges as authorized and when necessary.

10. Your Covered Component procedures will state whether it is permissible to use removable media (CD-ROMs, DVDs, USB keys, tapes, etc.) for storing ePHI.

11. Avoid duplicative storage of ePHI on devices by securely deleting or removing any unnecessary electronic copies.

12. Report to your HIPAA Contact or Information Security any unusual system activity including:
   a. Alerts displayed by a system or application indicating a problem;
   b. Unusual behavior such as seeming loss of control of mouse or keyboard; or
   c. Alerts displayed by security software meant to prevent malicious code, such as antivirus.

13. Report to your HIPAA Contact or Information Security potential security events such as:
   a. The loss of a device (personal or university-owned) that contains or has access to ePHI;
   b. The loss of a secondary authentication token, such as SecurID or Duo;
   c. Unusual account activity such as a last-login event occurring at an unusual time; or
   d. Someone accessing PHI that is not authorized to do so.

14. Media and devices containing ePHI must be disposed of properly, according to Information Security’s Media Destruction One Sheet. This means:
   a. Files on a computer system should be securely deleted, and
   b. Media must be physically destroyed by BU IS&T when no longer needed.

15. Only transmit or receive ePHI data when:
   a. Using Boston University’s wired or wireless network;
   b. Using an encrypted communication protocol, such as secure email (DataMotion), https, ssh, sftp, remote desktop, etc.; or
   c. After establishing a connection to via the Virtual Private Network (VPN) service.

Photographs, Audio and Video Recording of Patients
Most photos, audio recordings and video recordings of patients are stored electronically. Use the same safeguards as for any electronic PHI. When they are in a tangible form (e.g., a printout, x-ray or a photograph) follow the precautions listed above for Paper and Other Tangible PHI.
3. Using PHI in Treatment, for Payment and for Health Care Operations; Business Associates

3.1 Overview
The policies that follow describe routine and non-routine disclosures. Routine disclosures are those that are made regularly and frequently. For example, using PHI for treatment and to obtain payment for that treatment is a routine disclosure. PHI is also routinely used to manage the health care clinic. Detailed information on HIPAA’s rules for these routine uses is provided in these policies to facilitate the routine activities of the Covered Components.

Non-routine disclosures are rarely encountered. Information on HIPAA rules for non-routine disclosures is provided in policies 4 and 5, below. Covered Components are always encouraged (and in some circumstances required) to contact the BU HIPAA Privacy Officer for guidance and/or approval in these non-routine circumstances.

The disclosure policies also note when disclosures (both routine and non-routine) may or must be made without a written and signed Authorization.

3.2 Minimum Necessary Rule
In most circumstances, when using or disclosing PHI or when requesting PHI from another HIPAA Covered Entity/Component, the BU Covered Component must limit the use or disclosure to that which is necessary to accomplish the intended purpose of the use, disclosure, or request for information.

Exceptions to the Minimum Necessary Rule:
- Disclosures or requests by a health care provider of information for treatment purposes. Health care providers use their professional judgment in determining what PHI is needed for treatment purposes;
- Uses or disclosures pursuant to Authorization, because the disclosure should follow the patient’s direction in the Authorization;
- Disclosures made to the Secretary of Health and Human Services, which will be made by the BU HIPAA Privacy and/or Security Officers; and
- Uses or disclosures required by law, for example,
  - Mandatory reports of abuse, neglect or domestic violence,
  - Uses and disclosures for governmental health oversight activities,
  - Disclosures for judicial and administrative proceeding and pursuant to subpoena or court order.

In all other circumstances, follow the Minimum Necessary Rule.

3.3 Special Rules for PHI in Limited Data Sets
A Covered Component may use or disclose a Limited Data Set (defined below) only for the purposes of research, public health, or health care operations, and only after entering into a Limited Data Use Agreement with the recipient.
Definition of Limited Data Set
A limited data set is PHI that excludes the following direct identifiers of the individual or of the individual’s relatives, employers, or household members:

- Names;
- Postal address information, other than town or city, state, and zip code;
- Telephone numbers;
- Fax numbers;
- Electronic mail addresses;
- Social Security numbers;
- Medical record numbers;
- Health plan beneficiary numbers;
- Account numbers;
- Certificate/license numbers;
- Vehicle identifiers and serial numbers, including license plate numbers;
- Device identifiers and serial numbers;
- Web Universal Resource Locators (URLs);
- Internet Protocol (IP) address numbers;
- Biometric identifiers, including finger and voice prints; and
- Full face photographic images and any comparable images.

An alternate way of understanding a Limited Data Set is that it is PHI that has been de-identified except for dates, which may be included in a Limited Data Set. Thus, if you try to de-identify data but find you need to retain dates, treating it as a Limited Data Set may be a good option.

Limited Data Sets are frequently used in research.

Data Use Agreement
Contact the BU HIPAA Privacy Officer for a Limited Data Use Agreement either to be used in disclosing BU Covered Component PHI, or in receiving PHI from another entity.

BU researchers may accept Data Use Agreements from other entities disclosing research data to BU only if approved by the BU HIPAA Privacy Officer.

Breaches of Data Use Agreements
If a Covered Component that has disclosed its PHI pursuant to a Data Breach Agreement learns of the recipient’s possible breach of the agreement, the Covered Component must first report the matter to the BU HIPAA Privacy Officer, who will work with the Covered Component to take reasonable steps to investigate and, if necessary, cure the breach, end the violation, or discontinue disclosure of the data. If a breach is confirmed, the BU HIPAA Privacy Officer will make any necessary report to the affected individuals and the Secretary of Health and Human Services.

3.4 Patient Authorization Not Needed for Treatment Purposes
Treatment purposes includes providing, coordinating or managing a patient’s health care services.

Minimum Necessary Rule Not Applicable: When using PHI for Treatment purposes (including disclosing it to other providers for treatment purposes), it is not necessary to limit the use or disclosure to the “minimum necessary”. Health care providers should use their professional judgment in accessing, using and disclosing whatever information they deem necessary for treatment purposes.
**Research recruitment:** Anyone in a Covered Component may approach the Covered Component’s patients about participation in research, as that communication is considered part of treatment. However, the treating provider/Covered Component may not provide patient contact information or any other PHI to a researcher outside the Covered Component without the patient’s Authorization.

**Provider Treatment Recommendations, Options:** A face-to-face communication made by a Covered Component to an individual recommending additional services of the Covered Component or of another Covered Entity/Component falls within the definition of “Treatment.” For example, dentists may recommend use of a waterpik; dieticians may recommend certain foods or supplements. Providers and Covered Components are prohibited from accepting payment from any other entity or person to recommend that entity or person’s services or products to patients. See Section 4.2: Prohibited Uses of PHI.

### 3.5 Using PHI for Payment Purposes

**Disclosures for Payment Purposes**
An authorization is not required to use PHI for payment purposes. Payment purposes include all activities directed at obtaining reimbursement for health care services, such as:

- verifying an Individual’s insurance coverages;
- creating the claim;
- sending the claim to the patient and/or the patient’s insurer;
- interactions with the patient’s insurer for the purpose of obtaining payment;
- processing payments;
- collections activities; and
- evaluating an Individual’s eligibility for financial assistance.

**Minimum Necessary Rule Applies:** When using and disclosing PHI for payment purposes, only the minimum necessary information should be used and disclosed.

### 3.6 Using PHI for Health Care Operations Purposes

**Disclosures for the Covered Component’s Operations**
An authorization is not necessary to use PHI for the Covered Component’s operations, such as:

- quality assessment and improvement activities (but not generalized research);
- case management;
- human resources, including reviewing the competence and performance of providers and other Workforce members and resolution of internal grievances;
- training of professional and non-professional students;
- accreditation;
- certification;
- licensing;
- credentialing;
- financial management;
- compliance, risk management, auditing and legal services;
- investigations of possible fraud and abuse;
• business development and planning; and
• all other business and administrative activities required for the Covered Component to operate.

Minimum Necessary Rule Applies: When using and disclosing PHI for operations, only the minimum necessary information should be accessed, used or disclosed.

3.7 Routine Disclosures to an Individual’s Family and Friends
Patients are entitled to involve family and friends in their care, if they wish, and Covered Components should honor those wishes by disclosing PHI to those persons, to the extent the patient has involved them. Below is guidance on how to manage these disclosures in several types of circumstances in which this may arise.

Specific Authorization
If the patient signs an Authorization to disclose information to another person, the Covered Component should follow that Authorization. For example, if a patient signs an Authorization allowing a Covered Component to share billing and payment information with her spouse, the Covered Component should honor that Authorization, but may not go beyond it by providing the spouse non-billing/payment information.

Informal Authorization
If an Individual involves a friend or family member in his/her care, the Covered Component may disclose to that person information directly relevant to the nature of the person’s involvement with the patient’s care, even in the absence of a written Authorization. Providers may honor an Individual’s informal request to share his/her PHI with others if:

• the patient is present and requests the Covered Component do so, or
• if the patient is present and does not object, or
• if the provider reasonably infers from the circumstances, based on the exercise of professional judgment that the patient does not object to such disclosure.

For example, if a patient brings a friend to an appointment, it is permissible to discuss the patient’s condition, plan of care, and other matters typically discussed in such an appointment with the friend present. But it would not be permissible to provide that friend billing information, if the patient did not involve the friend in billing issues.

While providers may rely on a patient’s informal indication of permission to share information, having the patient indicate his/her desires in writing in an Authorization may help avoid confusion and misunderstanding.

Notification Purposes
The Covered Component may use or disclose PHI for purposes of notifying an individual’s family member, Legally Authorized Representative, or another person responsible for the care of the patient, of the patient’s location, general condition, or death. It may also use and disclose PHI in these circumstances for identifying or locating an individual’s family member, Personal Representative or other person responsible for the care of the individual.
3.8 Sharing PHI with the Patient’s Other Providers and Health Plans

Health care providers and health care plans often share information about the patients who are common to both. This is permissible under HIPAA, subject to the following:

**Treatment**

Treatment includes disclosing PHI to another health care provider who is treating the patient, or who may treat the patient, when the purpose of the disclosure is to provide, coordinate or manage treatment of the patient.

You do not need the patient’s Authorization or permission, but it is a good practice to require a patient to sign an Authorization when releasing records to another health care provider for Treatment purposes because that will confirm the patient’s relationship with the other provider. However, when that is not feasible, and when the Covered Component has a good faith belief that the other provider has, had or may be entering into, a treatment relationship with the patient, it is permissible to make the disclosure to the other provider without a signed patient Authorization.

*Minimum Necessary Rule Not Applicable*: Because this is considered using PHI for Treatment purposes, it is not necessary to limit the use or disclosure to the “minimum necessary”. Health care providers should use their professional judgment in accessing, using and disclosing whatever information each deems necessary for treatment purposes.

**Payment**

Disclosures to an Individual’s other health care providers and insurers for purposes of payment are permissible even without patient authorization. This covers all communications with a patient’s health plan and all communications with the patient’s other health care providers when the purpose relates to payment for health care services of one or more of them.

*Minimum Necessary rule applies.*

**Disclosures for Operations of Other Providers and Covered Components/Entities**

HIPAA allows a Covered Component to disclose PHI to another Covered Entity/Component for the operations of that other Covered Entity/Component, but only when all of three of the following apply:

- Each Covered Entity/Component has or had a relationship with the patient whose PHI will be shared; and
- The PHI pertains to that relationship; and
- The disclosure is for one of the purposes listed below:
  - Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines (but not research); population-based activities relating to improving health or reducing health care costs; protocol development; case management and care coordination; contacting health care providers and patients with information about treatment alternatives; or
  - Reviewing the competence or qualifications of health care professionals; evaluating practitioner and provider performance; reviewing health plan performance; conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers; training of non-health care professionals; accreditation; certification; licensing or credentialing activities; or
For the purpose of investigating health care fraud and abuse.

The Minimum Necessary rule applies.

This does not occur very often, and Covered Components are encouraged to contact the BU HIPAA Privacy Officer for guidance.

3.9 Disclosing PHI to Business Associates

BU’s Covered Components may engage, or BU may engage on behalf of the Covered Components, entities outside of BU to perform various services. When the services involve the outside entity accessing, using, creating or disclosing PHI held by any Covered Component, those entities are likely to be Business Associates of the Covered Component. The University, including its Covered Components, may not disclose any PHI to Business Associates until a Business Associate Agreement is fully executed.

Business Associate Agreements

The Business Associate Agreement must contain certain elements, which require the Business Associate to maintain the confidentiality of the PHI that it receives, to use and disclose such information only for the purposes for which it was provided, and to comply with the same HIPAA requirements as the Covered Component.

Responsibilities

The Office of the General Counsel, in consultation with the BU HIPAA Privacy Officer will:

- Approve a standard form Business Associate Agreement and make it available to the Covered Components and Support Units; and
- Approve any changes to a Business Associate Agreement.

The BU HIPAA Privacy Officer will:

- Be available to advise Covered Components and Support Units on whether a service provider is a Business Associate; and
- Periodically audit the Business Associate logs and agreements maintained by Covered Components and Support Units.

The Covered Components are responsible for:

- Determining whether any service provider it retains, who is external to BU, is a Business Associate, and if so, for ensuring a Business Associate Agreement approved by the BU HIPAA Privacy Officer is fully executed before any PHI is disclosed;
- Contacting the BU HIPAA Privacy Officer to approve any change the terms of the standard approved Business Associate Agreement; and
- Maintaining on the BU HIPAA SharePoint site a log of all Business Associates and copies of all Business Associate Agreements for that Covered Component.

Support Units that retain the services of a Business Associate are responsible for:

- Determining whether the service provider is a Business Associate and if so, entering into a Business Associate Agreement before disclosing any PHI. The Covered Component HIPAA Contact will act as a check and upon becoming aware of a Business Associate retained by a Support Unit, will verify that a Business Associate Agreement was fully executed.

Who is a Business Associate?

HIPAA defines a Business Associate as a person or entity that:

- is not a member of the Covered Component Workforce,
• provides a service, or performs a function, or assists in the performance of a function or activity on behalf of a Covered Component, and
• in performing its duties for the Covered Component, may access, use, create or disclose PHI.

HIPAA does not define which entities or services fall into the Business Associate category; the determination must be made case by case, using the definition above. Following are examples:

<table>
<thead>
<tr>
<th>Almost Always A Business Associate</th>
<th>May Be A Business Associate (when services involve PHI)</th>
<th>Never A Business Associate</th>
</tr>
</thead>
<tbody>
<tr>
<td>Claims processing or administration</td>
<td>Management consultants</td>
<td>Members of the Covered Component’s Workforce</td>
</tr>
<tr>
<td>Billing</td>
<td>Legal services</td>
<td>Other health care providers of the Covered Component’s patients, when acting in that capacity; i.e., a health care provider providing health care services. Note that health care providers may perform business services such as billing or consulting for a BU Covered Component; in which case it would be a BA. See column to the left.</td>
</tr>
<tr>
<td>Practice management</td>
<td>Financial, accounting, actuarial, and similar services</td>
<td>Custodians, janitors, couriers, repairmen etc. where access to PHI is not required to perform their services, even if there may be incidental disclosure to them</td>
</tr>
<tr>
<td>Data analysis, processing or administration</td>
<td>Data aggregation services, IT services</td>
<td>Financial institutions processing financial transactions (e.g., credit card processing or check clearing)</td>
</tr>
<tr>
<td>Utilization review</td>
<td>IT services, including data migration or software or system maintenance</td>
<td>Public health oversight agencies, such as the Massachusetts Department of Public Health, performing health oversight functions</td>
</tr>
<tr>
<td>Quality assurance</td>
<td>Collection agencies</td>
<td>Recipients of De-Identified Information or “Limited Data Set”: No Business Associate Agreement is needed when the health information being disclosed or created has been de-identified in accordance with the de-identification standards under the Privacy Regulations, or the health information qualifies as a Limited Data Set disclosed pursuant to a Limited Data Use Agreement</td>
</tr>
<tr>
<td>Almost Always A Business Associate</td>
<td>May Be A Business Associate (when services involve PHI)</td>
<td>Never A Business Associate</td>
</tr>
<tr>
<td>-----------------------------------</td>
<td>-------------------------------------------------------</td>
<td>---------------------------</td>
</tr>
<tr>
<td>Transcription services, answering services</td>
<td>Accreditation organizations</td>
<td>Health care insurers of the Covered Components’ patients, when acting in that capacity; Disclosures to health care insurers is allowed for Payment purposes.</td>
</tr>
</tbody>
</table>

**Enforcement of Business Associate Agreements**

If the Covered Component becomes aware of any breach of a Business Associate Agreement, it must notify the BU HIPAA Privacy Officer to assess whether it is necessary to take steps to cure the breach or terminate the underlying service contract if feasible.

**Standard Form**

The approved BU standard form of Business Associate Agreement should be used.

If an outside organization or person sends its own form of Business Associate Agreement to be signed, please inform the BA that the PHI belongs to BU and its patients and BU protects it by using its own form. If the Business Associate insists on using its form or requests modifications of the BU template, contact the BU HIPAA Privacy Officer.

**BU as a Business Associate**

If any Boston University office or department provides services to an outside HIPAA Covered Entity such that the outside entity requests BU sign a Business Associate Agreement, contact the BU HIPAA Privacy Officer, who will determine whether a Business Associate Agreement is needed and if so, may approve it.
4. Uses Required or Permitted by Law; Prohibited Uses of PHI;

The situations described below do not occur routinely, and there are a variety of conditions on these types of disclosures. Therefore, the Covered Components should refer any such requests for disclosure to the BU HIPAA Privacy Officer and should not respond on their own.

4.1 Required by Law

**Immunizations Records Provided to Schools:** Because schools are required by law to obtain certificates of vaccination, Covered Components may send such records to a school upon request by a student or parent. No written Authorization is needed;

**Other Types of Disclosures That May Be Authorized**

Please contact the BU HIPAA Privacy Officer if you receive any of the following types of requests for disclosure of medical records. They can assist in ensuring the request is allowed under the law, and that the response to the request and any disclosure fulfills BU’s legal obligations.

**Responsibilities of Covered Components:**

- Recognize these circumstances when they occur;
- Contact the BU HIPAA Privacy Officer promptly for guidance; and
- Keep record of any such disclosures on a form provided by the BU HIPAA Privacy Officer.

**Responsibilities of Privacy Officer:**

- BU HIPAA Privacy Officer will respond promptly to notification from Covered Component of any requests for disclosure of PHI; and
- BU HIPAA Privacy Officer will authorize and coordinate any disclosures of PHI and will make or coordinate any communications necessary to the requestor.

**Disclosures Required by Law:** If a Disclosure is required by Law, the Covered Component will comply with the law. We do not need to obtain patient Authorization and may not refuse to comply with the law because the patient has not authorized the disclosure. Examples include:

- Public Health Activities;
- A Public Health Authority (including the Massachusetts Department of Public Health (“DPH”) and the Centers for Disease Control) that is authorized by law to collect or receive information for the purpose of preventing or controlling disease, injury, or disability. Typical mandatory reports include reporting certain diseases and injuries; participating in public health surveillance and public health investigations and interventions;
- Reports of child abuse or neglect to the Massachusetts Department of Children and Families and similar public agencies;
- Mandatory reports to the federal Food and Drug Administration (FDA); and
- Reports of certain reportable communicable diseases to the Massachusetts DPH (or similar agencies).

**Disclosures Permitted by Law:** In addition to the mandatory reports referenced above, Covered Components may, if they wish, disclose PHI without any patient Authorization in reporting:

- Abuse, neglect and/or domestic violence (partner violence) when the Individual agrees to the Disclosure or when the Disclosure is authorized by statute or regulation;
• To a health oversight agency for oversight activities authorized by law to oversee the provider or government benefit programs for beneficiary eligibility determinations, and to governmental agencies charged with determining compliance with program standards or civil rights laws, when the PHI is necessary for the oversight;
• To a court or administrative tribunal order or in response to a subpoena, discovery request, or other lawful process; such disclosures are managed by the Office of the General Counsel;
• To Law Enforcement for any of the following purposes:
  o When the subject of the Disclosure is an Individual who is or is suspected to be a victim of a crime, abuse, or other harm;
  o In response to a court order or court-ordered warrant, or a subpoena or summons issued by a judicial officer or a grand jury subpoena;
  o In response to an administrative subpoena or summons, a civil or an authorized investigative demand when the information sought is relevant to a legitimate law enforcement inquiry;
  o For the purpose of identifying or locating a suspect, fugitive, material witness, or missing person;
  o For the purpose of alerting law enforcement of the death of the Individual, if the Covered Component has a suspicion that such death resulted from criminal conduct; and
  o Based on a good faith belief that the PHI disclosed constitutes evidence of criminal conduct that occurred on Covered Component premises;
• Based on a good faith belief that the Disclosure is necessary to prevent or lessen a serious imminent threat, including to the target of the threat, or is necessary for law enforcement authorities to identify or apprehend an Individual under specified circumstances;
• For certain military and veterans’ activities, national security and intelligence activities, and to correctional institutions, as specified in applicable regulations;
• To workers’ compensation programs that provide benefits for work related injuries or illness; and/or
• To the Secretary of Health and Human Services (HHS) information that is pertinent to ascertaining compliance with the privacy requirements.

4.2 Prohibited Uses of PHI: Marketing; Sale; non-BU Purposes

Personal Use or Disclosure of PHI
Workforce members may access, use and disclose PHI only as stated in these policies and in the Covered Component’s Notice of Privacy Practices. Use and disclosure for personal purposes, or to benefit someone other than the patient and the BU Covered Component, is prohibited. For example:

• Workforce members may not post any information, photos, videos or anything else about a patient on social media; and
• Workforce members may not discuss patients, their conditions, treatment or other information, with family members and close friends who are not part of the patient’s care team.
Sale of PHI Prohibited
BU will not disclose any PHI for financial remuneration (i.e., direct or indirect payment from the party whose product or service is being marketed) unless the arrangement activity is approved in advance by the BU HIPAA Privacy Officer.

Marketing Defined
Marketing is any communication about a product or service that encourages recipients of the communication to purchase or use the products or services of a person or entity that is outside of the Covered Component.

Marketing does not include medical advice and recommendations of a treating provider. That is considered “treatment.” See Policy 3, Routine Use and Disclosure of PHI.

Marketing also does not include informing patients about services offered by a Covered Component. For example, the Danielsen Institute could inform a patient who has regular individual therapy that the Institute also offers group therapy sessions that the individual may wish to consider taking. That communication is allowed as part of Treatment. However, because each Covered Component is separate, if the Danielsen Institute were to recommend dental care at the GSDM Dental Clinic; that would constitute marketing.

Using PHI for Marketing Prohibited
BU Covered Components do not market the products and services of companies or persons to their patients, and do not use or disclose their patient PHI (including lists of patients and their contact information) for marketing purposes, unless the patient has signed a properly completed written authorization and the BU HIPAA Privacy Officer has approved the activity.

Covered Component Workforce members may not market products and services to Covered Component patients; for example, if a Workforce member sells supplements, or kitchenware, or cosmetics, s/he may not use work time to market those products and may not discuss those products with any Covered Component patient.

Activities Which Are Not “Marketing”
Marketing does not include activities for patient treatment, such as:
- Prescription refill reminders;
- Communications about a drug or biologic that is prescribed for or recommended to the patient; or
- Activities involved in treatment of the patient by a health care provider, including communicating the Plan of Care; prescribing a course of medication; case management or care coordination; or to direct or recommend conventional or alternative treatments, therapies, health care providers, or settings of care to the patient.

4.3 Fundraising and Promotion
PHI includes patient demographics and contact information. Thus, a mailing list of current and/or former patients is PHI.

Covered Components may not use any PHI to solicit donations unless the BU HIPAA Privacy Officer and the Senior Vice President for Development and Alumni Relations are consulted and agree on the PHI that may be accessed and used, consistent with HIPAA.
BU and/or certain Covered Components may wish to use images of patients and/or patient information in promoting BU and/or the Covered Component. This is permissible if the individual patient signs an appropriate Authorization. Contact the BU HIPAA Privacy Officer before proceeding.
5. Situations in which Authorizations are Necessary

5.1 General Rules on Authorization

When an Authorization is Required
If you are not using/disclosing PHI for treatment, payment or to manage the clinic as described in Policy 3 or for reasons that are required or permitted by law, then the patient must sign a written Authorization allowing you to use/disclose the patient’s information.

BU’s Authorization Form
Each Covered Component has an Authorization form approved by the BU HIPAA Privacy Officer which contains the elements required by HIPAA. These are found at http://www.bu.edu/hipaa/forms-for-health-care-providers/. Contact the BU HIPAA Privacy Officer if you want to change the language of the Authorization form for any reason.

Other Entities’ Authorization Forms
Covered Components may accept and comply with authorizations on BU’s standard form, if sufficient information is provided. If the Covered Component receives an Authorization that is on a form other than the standard BU Authorization, Covered Components may accept the Authorization if it contains the same elements as BU’s Authorization and is consistent with this Policy. Questions about the validity of an Authorization can be directed to the BU HIPAA Privacy Officer for guidance.

Using the Authorization Form
Below are instructions on the use of the Authorization form. Any questions about whether an Authorization form is needed or about using the form should be directed to the BU HIPAA Privacy Officer.

When completing the Authorization or reviewing Authorizations, please keep the following in mind:

- The information to be used or disclosed must be identified with enough specificity to allow the Covered Component to comply.
- The name or other specific identification of the person or entity the information should be disclosed to must be provided. (e.g., “send a complete copy of my records dated 1/1/2016-7/1/2016 to Dr. Laura Smith at [address]”; or “to Boston Medical Center”).
- A description of the reason for the use or disclosure (e.g., “at the request of the individual,” or “for follow up care” or “for personal use”).
- An expiration date or an expiration event must be provided (e.g., “this Authorization expires in six months;” “12/31/2016;” or “at the end of the research study”).
- The individual whose PHI is to be used or disclosed must sign and date the Authorization. If someone other than the individual is authorized to sign, that person’s capacity should be noted (e.g., “Guardian” or “Mother of minor child”). See Policy 5, Section 5.2 and Section 5.3 for more information.
- The Covered Component is responsible for maintaining signed Authorizations for six (6) years.
- The Minimum Necessary Rule does not apply to disclosures based on patient Authorization. Rather, the Covered Component should disclose documents requested in the Authorization.
Defective Authorizations
Authorizations are defective and invalid if any material information in the Authorization is known to the Covered Component to be false or if any of the following other defects exist:

- The expiration date has passed, or the expiration event is known by The Covered Component to have occurred;
- The Authorization has not been filled out correctly or completely;
- The Authorization is known by The Covered Component to have been revoked; or
- The Authorization violates the prohibition on conditioning of Authorizations, as described immediately below.

Questions should be directed to the BU HIPAA Privacy Officer.

Prohibition on Conditioning of Authorizations
We may not condition the provision of treatment on the patient’s signing an Authorization, except when the patient is participating in a clinical research trial. If the Authorization is required for disclosures related to the research, then the researchers may condition enrollment in the clinical trial on the Individual signing an Authorization for disclosures needed for the clinical trial.

HIV Tests and Results
Covered Components may report the results of HIV tests without patient authorization to the individual tested and to the Massachusetts Department of Health for infectious disease surveillance.

In all other circumstances, Covered Components may disclose the fact of HIV testing or HIV test results only after receiving the patients’ written authorization for that disclosure. Each release of HIV test results must be authorized by a separate written authorization.

Genetic Information
Covered Components whose medical records include genetic information about an individual may not disclose that genetic information to anyone other than the individual tested, except (i): upon written consent of the individual; or (ii) upon proper judicial order; or (iii) for research purposes, in compliance with the policies for use and disclosure of PHI for research purposes. See Section 5.5, Accessing and Using PHI for Research.

Revocation of an Authorization
A person who has signed an Authorization may revoke it at any time by providing a written notice of revocation to the Covered Component. When an individual revokes his/her Authorization, the Covered Component may no longer rely on the revoked Authorization. However, the revocation does not affect disclosures that were made pursuant to the Authorization prior to receiving the Revocation.

Authorization Not Needed to Disclose Immunization Information to a School
Massachusetts schools are required by law to obtain immunization records for students. Mass. General Laws Chapter 76, Section 15. Therefore, we do not need to obtain and Authorization to provide information on immunizations to any school.

Release of Information Practices
Each Covered Component will adopt procedures for release of information.
5.2 Parents, Guardians and Minors

General rules:

1. Adults age eighteen (18) and older make their own decisions on their rights under HIPAA and sign their own Authorizations.
2. Persons under the age of 18 are minors. A parent of the minor makes decisions for the child and signs the child’s Authorization. The parent should note his/her capacity, e.g., “mother/father/parent” on the Authorization.

Exceptions to both of these general rules are described below.

Minors and their Parents
A Covered Component may assume either parent of a child under age 18 is authorized to sign Authorizations for the child, unless they have knowledge of a court order that has limited or taken away a parent’s authority.

When parents are divorced, the fact that one parent has full custody does not mean that the other parent’s authority has been limited; a court order would state any such restriction.

If a Covered Component has reason to believe a parent who wishes to make decisions for, and sign Authorizations on behalf of, a minor child is not authorized to do so, the Covered Component should request a copy of the court order restricting a parent’s rights and/or specifying who may make decisions regarding the minor’s health care and who may sign Authorizations for the child. Questions may be directed to the BU HIPAA Privacy Officer or the Office of the General Counsel.

Emancipated Minors
Massachusetts law includes the Emancipated Minor statute which allows health care providers to provide treatment to minors (persons who have not attained the age of eighteen) based on the Informed consent of the Emancipated Minor.

Reasons for emancipation include:

- The minor is married, widowed or divorced;
- The minor is the parent of a child, in which case s/he may also give consent to medical or dental care of his/her child;
- The minor is a member of any of the armed forces;
- The minor is pregnant or believes herself to be pregnant;
- The minor is living separate and apart from his/her parent or legal guardian, and is managing his/her own financial affairs; or
- The minor reasonably believes him/herself to be suffering from or to have come in contact with any disease defined by the Massachusetts Department of Health as dangerous to the public health. However, the minor may only consent to care which relates to the diagnosis or treatment of that disease.

Note that a minor may not consent to an abortion or sterilization, even if Emancipated.
**Drug Dependent Minors**
Under Massachusetts law, a minor twelve years of age or older who is found to be drug dependent by two or more physicians may give consent to hospital or medical care related to the diagnosis or treatment of such drug dependency. The consent of the parent or legal guardian of such minor is not necessary to authorize hospital and/or medical care related to drug dependency.

**When Parent or Legal Guardian agrees to confidentiality**
If a parent or legal guardian has signed an agreement of confidentiality between the provider and the minor with respect to health care service, then the parents/legal guardian are not authorized to make decisions for the minor for the matters covered by the Agreement, and any Authorization for disclosure must be signed by the minor.

**Verifying Identify When Releasing Records**
The Covered Component is responsible for verifying the identity of the person requesting PHI and the authority of such person to have access to the PHI or to authorize its disclosure.

If the person is known to the Covered Component, and there is no question as to his/her authority, the Covered Component may accept the signed Authorization from the known person. This commonly occurs when a patient over the age of 18 who has not been found incompetent signs his/her own Authorization; when a parent of an unemancipated minor is known to the Covered Component based on the parent’s involvement in the minor’s care signs for the minor patient; and when the Covered Component has previously verified the legal status of a guardian or other representative.

If the person requesting records or presenting an Authorization is not known to the Covered Component, the Covered Component must make reasonable efforts to verify the person’s identity and authority. Following are common ways of verifying:

- Check the requesting party’s picture identification;
- Verify that the address to which the records are requested to be sent is the address of record of the individual; and/or
- Obtain a copy of a court appointment or other document that authorizes access to the PHI under law (such as a letter from the Department of Public Health authorizing the disclosure).

The Covered Component may rely on documents presented that appear to be legitimate on their face. Any questions regarding a person’s authority to obtain PHI should be directed to the BU HIPAA Privacy Officer.

**5.3 Legally Authorized Representative of an Adult Patient**
If an adult is not competent to make his/her own decisions, a Legally Authorized Representative may exercise the patient’s rights and sign Authorizations on behalf of the patient.

Legally Authorized Representatives may hold a variety of titles, including Personal Representative, Guardian; Conservator, Substitute Decision Maker, Health Care Agent, and others; for simplicity, the term Legally Authorized Representative is used in these policies. When a Legally Authorized Representative (by whatever title) signs an Authorization on behalf of the patient, the Covered Component must verify the authority of the Legally Authorized Representative, typically by obtaining the court order, administrative tribunal order, or appointment document. Legally Authorized Representatives usually have these documents readily available. Any questions about the authority of a
Personal Representative should be directed to the BU HIPAA Privacy Officer or Office of the General Counsel.

**Appointment of Health Care Agent**

If an adult patient has appointed a health care agent in accordance with Massachusetts law and the adult has subsequently been found incapacitated and incapable of making or communicating health care decisions by a physician, Authorizations must be handled as follows:

a. Obtain a signature on the Authorization from the health care agent, not from the patient.

b. A copy of the health care proxy form listing the agent’s name must accompany the request and be filed with the Authorization and request for PHI.

c. If multiple parties have been named as agent, obtain Authorization from all parties. If, the proxy lists “Party A” OR “Party B,” the Authorization of either is sufficient.

d. The Covered Component must observe the terms of the appointment. If the individual regains mental capacity, the health care proxy is rendered ineffective and then signature of the proxy on an Authorization does not suffice. Instead, the individual must then sign any Authorization.

e. Take care not to disclose PHI based on the Authorization of the health care agent if you have no corroborating evidence that the individual has been declared incapacitated by a physician as required by Massachusetts law.

Contact the HIPAA Privacy Officer or Office of the General Counsel with any questions.

**5.4 After a Patient’s Death**

PHI of deceased individuals remains protected under HIPAA for 50 years following the date of death.

**Who can authorize a release of the records of the deceased?**

If the individual is deceased, the Covered Component must obtain the Authorization from the court-appointed administrator or executor of the decedent’s estate. If the Covered Component is unable to obtain the court order naming the administrator or executor, or if an administrator or executor has not been appointed, contact the BU HIPAA Privacy Officer or the Office of the General Counsel.

**Family and Friends Rights to Records**

If a family member (or friend) was involved with an individual’s care during his/her life, we may release the individual’s records upon Authorization by that person, just as we shared the patient’s PHI with the involved family member during the patient’s life.

If the person requesting records of a deceased patient was not involved in the patient’s care during the patient’s lifetime, then only a legally authorized representative of the estate may authorize release of the patient’s medical records. The Covered Component should receive a court order nominating the person as a Personal Representative or Executor of the deceased patient’s estate before releasing records of a deceased person.

A deceased patient’s surviving spouse, children, family members, friends and others are not authorized to request and receive the deceased patient’s PHI simply by virtue of the family relationship.
Disclosing Records of Deceased Individual for Research Purposes
Please see the next Section, 5.5: Accessing and Using PHI for Research.

5.5 Research: Authorizations and Waivers

Research is not one of the purposes for which PHI may be used without patient Authorization (Treatment, Payment or Health Care Operations (see Policies 3.4, 3.5, 3.6) and so Covered Components may not allow access to its PHI for research purposes unless the researcher has obtained and presented to the Covered Component HIPAA Contact:

(i) Institutional Review Board (IRB) approval and
   a. Authorizations signed by each patient whose information is requested, or
   b. An IRB Waiver of patient Authorization
(ii) in the case of Activities Preparatory to Research, an acceptable attestation. A form for this purpose is found at http://www.bu.edu/hipaa/forms-for-health-care-providers/

In order for Covered Components to determine whether it is permissible to release PHI to a researcher, the HIPAA Contact must determine the following:

• Is the activity for which PHI is requested “research” under HIPAA?
• If so, is the researcher authorized to receive the PHI requested?

What is Research under HIPAA?

HIPAA defines “research” as an activity intended to lead to generalizable knowledge.

Quality assurance activities conducted by the Covered Component solely for its internal purposes (e.g., to assess or improve the quality of care provided to patients/clients) is not “research” but instead falls within “operations” and is generally permissible without the individual’s Authorization; the rules for using PHI in research will not apply because it is not research.

Access to PHI for research purposes

Authorization: The Covered Component may permit access to PHI for research if an Authorization for such access has been received from the individual or individual’s representative.

IRB Waiver of Authorization:
The Covered Component may permit access to PHI for research without an Authorization if a Waiver of Authorization has been obtained from an IRB. A form is available for this purpose.

Special Rules for Activities Preparatory to Research:
Researchers often need to access PHI in order to get sufficient information to design a study, evaluate the feasibility of a study, or otherwise prepare for research. This typically takes place in advance of presenting the study to the IRB or seeking financial support for the study.

Researchers may not access any PHI for these purposes unless:

(i) the patients have explicitly authorized such activities, e.g., in an authorization signed to allow the creation of a data repository; or
(ii) the researcher completes a Waiver Preparatory to Research form, attesting to certain security and privacy measures, such as:
(a) the researcher seeks the PHI solely to prepare a research protocol or for similar purposes preparatory to research;
(b) The researcher will access only the PHI necessary for this purpose;
(c) The researcher will not remove any PHI from the premises of the Covered Component.

Special Rules for Access to Records of Decedents for Research Purposes:
A Covered Component may permit access to PHI for research if the Covered Component’s HIPAA Contact receives from the researcher:

- a representation that the use or disclosure sought is solely for research on the PHI of decedents;
- documentation, at the request of the Covered Component, of the death of such individuals; and
- a representation that the PHI sought is necessary for the research.

Covered Components may accept such a statement from a researcher if it has been reviewed and approved by the IRB.

Research Data Repositories Containing PHI

Creating Data Repository from PHI: If a Covered Component wishes to create a repository of information from clinical records for a specific study or potential future research, the creation must be approved by the IRB and by the BU HIPAA Privacy Officer. This will ensure that patients properly authorize the inclusion of their information in the database, or that a waiver has been approved. If the repository contains only a Limited Data Set, its use can be governed by a simple Data Use Agreement, which

Using the PHI in an approved Data Repository:
Use of data in a repository must be separately approved by the IRB for each study.

5.6 Students and Observers

Trainees:

Students enrolled in one of BU’s health schools who participate in patient care within a Covered Component as part of their training are part of that Covered Component’s Workforce. However, there are restrictions on their use of PHI in their education, and on faculty use of patient PHI in education.

PHI, including excerpts from the patient medical record, images, and factual summaries, may be used for educating students only as follows:

- If the PHI is fully de-identified by absence of the 18 identifiers (see Policy 1 HIPAA Basics, Section 1.4: De-Identified PHI), it can be used without an Authorization. For example:
  - a faculty member or student may use an x-ray image if all identifying information is redacted, as the image itself does not identify the individual;
  - A faculty member or student may describe the health condition of a specific patient who suffered complications following standard treatment if the minimum necessary rule is followed, and the information is de-identified.
- All other uses of PHI in education require a signed Authorization.
Students who do not participate in patient care are not part of the Covered Component Workforce. See next section on Shadowing.

**Shadowing, Observers**
Covered Components that choose to allow students and others to “shadow” patient care as Observers must document a procedure for approving the shadowing as part of the Covered Component’s education mission (e.g., prospective students) or health care operations (e.g., a prospective faculty member or employee allowed to shadow as part of the recruiting process).

If allowed, the following safeguards must be in place:

- Patients must be told who the person shadowing is and given an opportunity to object to their presence. If a patient objects, the Observer must leave the patient’s area;
- Observers may not interfere with patient care;
- Observers may not participate in any way in patient care; and
- Observers must sign an attestation in advance of the shadowing experience confirming their health status, as required by the Covered Component, and their understanding of the confidentiality of all patient care information. Observers are not members of the Workforce and are not required to complete HIPAA training.


**5.7 Using PHI in Publishing**
Publishing case reports and articles in professional journals is an important part of the educational mission of the University. Faculty, residents and students in BU Covered Components may wish to write about the diagnosis, treatment, response to treatment, and follow-up after treatment of one or more individual patients (“Articles”). The usual rules apply:

- If the case report uses only de-identified data (see Section 1.4: De-identified PHI) then it is permissible under HIPAA to use the information for the case report without the patient’s Authorization.
- If some of the 18 identifiers remain in the Article, it would not meet the above standard for De-identification. There is an alternate method of de-identification: the author does not wish to obtain an Authorization and believes the information in the case not cannot be used to identify any individual, s/he may contact the BU HIPAA Privacy Officer, who will review the matter and may obtain an expert opinion on De-identification. Send the case note or article to hipaa@bu.edu for review.
- If the information used is not de-identified in one of the ways described above, the author will be required to obtain a signed HIPAA authorization from the patients (or their legally authorized representatives) for the use and disclosure of their PHI in the Case Note.

Please always consider obtaining patient authorization for the use of the PHI, given reports in the press of patients who have been upset upon recognizing themselves, or upon being recognized by others despite use of only de-identified PHI.

A special-purpose Authorization is available for this purpose at http://www.bu.edu/hipaa/forms-for-health-care-providers/ See also HRRP policies on the IRB’s role in approving case series.
6. Individuals’ rights under HIPAA

6.1 Right to Notice of Privacy Practices

Forms for each of the rights described in this section are available at http://www.bu.edu/hipaa/forms-for-health-care-providers/

Notice of Privacy Practices
Patients have the right to be informed of the uses and disclosures of their PHI that may be made by the Covered Component, and of their rights and the Covered Component’s responsibilities under HIPAA. To this end, each Covered Component is required to have a Notice of Privacy Practices (“NPP”) approved by the BU HIPAA Privacy Officer. Under Massachusetts law, Covered Entities must include in their NPP a notice of the Covered Component’s records retention and destruction policy for its medical records.

Posting the NPP
The NPP must be posted in an area where patients will see it.

If the services of the Covered Component are described on any website, the Covered Component shall also ensure the approved NPP is prominently posted on the Covered Component’s website.

Providing NPP to Patients
The Covered Component must provide a copy of its NPP to patients no later than the first date the Covered Component provides health services to the individual.

1. If the first contact with the individual is electronic, notice must be furnished contemporaneously with the electronic transmission.
2. If the first contact with the individual is via telephone, the Notice must be provided upon the first service delivery date.
3. If it is impossible or impracticable to provide the Notice due to an emergency situation involving the individual, the Covered Component may provide the NPP as soon as reasonably practicable after the emergency situation has passed.

The Covered Component must make a good faith effort to obtain written acknowledgement from the individual of his/her receipt of the NPP. If the Individual declines to sign the acknowledgment for any reason, the Workforce member who offered the NPP shall document that s/he offered it, and that the Individual declined to sign. The Acknowledgment form shall be placed in the Individual’s medical record.

In addition, Covered Components must make copies of the NPP available to any Individual who requests one at any time.

6.2 Right to Access and Copy Own Health Record
Except in limited circumstances described below, individuals have the right to access, inspect and receive a copy of PHI about them in the Covered Component’s Designated Record Set.
Use of Authorization Form
A written request is not legally required in order to provide copies of the Designated Record Set, in whole or in part, to the patient to obtain his/her own information. However, a written request on BU’s approved Authorization form allows the Covered Component to ensure that it is providing what the individual wishes to have and is doing so in a timely manner.

Approved Authorizations are found at http://www.bu.edu/hipaa/forms-for-health-care-providers/

When complete medical records are requested, the Covered Component should refer to its Designated Record Set procedure when a request for PHI is received to ensure disclosure of all documents subject to disclosure.

Time Period to Respond and Provide Access
Requests for records for the purpose of a claim or appeal under any provision of the Social Security Act or any federal or state financial needs-based benefit program must be furnished within 30 days pursuant to Massachusetts law, without any extension of time.

All other requests should be fulfilled as soon as practicable. If the Covered Component is not able to provide the requested records or respond to the request within 30 days, the Covered Component shall contact the BU HIPAA Privacy Officer and the BU HIPAA Privacy Officer may provide the Individual written notification of the reasons for the delay and the expected date of fulfilling the request.

Format of Records
The Covered Component shall provide the information requested in the format requested by the individual, if reasonably possible. The BU HIPAA Security Officer is available to advise on producing PHI in an electronic format. The Covered Component shall contact the BU HIPAA Privacy Officer in the event it is not able to accommodate the individual’s preferred format.

Inspection or Summary in Lieu of Copies
If the individual requests inspection of the records rather than a copy, the Covered Component shall arrange for a mutually convenient time and place for the individual to inspect the Designated Record Set.

The Covered Component may provide an individual with a summary or an explanation of the PHI requested, in lieu of providing access to the PHI, if the individual:

- agrees in advance to the summary; and
- agrees in advance to any fees imposed (if any) by the Covered Component for preparation of the summary.

Clarification of Request Permitted
The Covered Component may discuss the scope, format, and other aspects of the request for access with the individual, as necessary to facilitate the timely provision of access or copies.

Charges for copies
1. No fee may be charged to a patient who requests his/her record for the purpose of supporting a claim or appeal under any provision of the Social Security Act or any federal or state financial needs-based benefit program.
2. Covered Components will document in their procedures whether it will charge for other copies. Any charges must comply with the following:

*Electronic copies:* Covered Components may charge a flat fee of $6. If a Covered Component receives a request for electronic copy of a record which will entail an unusual amount of work, the HIPAA Contact shall contact the BU HIPAA Security Officer for guidance;

*Paper copies:* Covered Components may not charge a flat fee for paper copies. Any charges must be reasonable and based on the labor and supply costs of copying.

**When Requests for PHI May be Denied**

*Grounds for Denial:*
The Covered Component may deny an individual access to PHI in certain limited situations. Before denying access or copies, the Covered Component shall notify the BU HIPAA Privacy Officer, who will assist in ensuring the Covered Component fulfills its obligations under HIPAA, including written notification to the individual of the Covered Component’s decision.

*Unreviewable Ground for Denial* – The Covered Component may deny an individual access, in whole or in part, without providing the individual an opportunity for review, in the following circumstances:

- Records requested are not in the Designated Record Set (e.g., Psychotherapy Notes);
- The individual is an inmate, care was provided in the penal institution, and the information requested could jeopardize the health, safety, security custody or rehabilitation of the inmate or others;
- The individual has consented to participate in a clinical research project and the requested information is restricted during the course of the research; and
- Information requested was obtained from someone other than a healthcare provider under a promise of confidentiality (for example, if the healthcare provider documented in the record concerns and information provided by a family member of the individual after a promise of confidentiality).

*Reviewable Grounds for Denial:*
Denials of access based on reasons listed below are subject to review by a licensed healthcare professional who was not involved in the original decision to deny access, upon the written request of the individual. Reviewable grounds for denial include:

- Denials made by a licensed health care professional who has determined that the access requested is likely to endanger the life or physical safety of the individual or others;
- PHI that makes reference to another person (unless such other person is a health care provider) and a licensed health care professional has determined, in the exercise of professional judgment, that the patient’s access to that information is reasonably likely to cause substantial harm to such other person; or
- Denial of a request for access made by the individual’s personal representative when a licensed health care professional has determined, in the exercise of professional judgment, that the provision of access to such personal representative is reasonably likely to cause substantial harm to the individual or another person.
Procedure when Request Is Denied
The Covered Component and BU HIPAA Privacy Officer shall notify the individual in writing of the denial, including:

- An explanation/reason for the denial; and
- A statement of the individual’s rights and instructions on:
  - How to request a review by a licensed health care professional (if applicable);
  - Filing a complaint with the Covered Component’ HIPAA Contact; and
  - Filing a complaint with the United States Secretary of Health and Human Services.

In the case of denials subject to review, if an individual submits a written request for a review, the Covered Component shall:

- Designate a licensed health care professional who did not participate in the original decision to deny access as the reviewing official.
- Ensure review by the reviewing professional within a reasonable period of time.
- Promptly provide written notice to the individual of the determination of the reviewing professional, and take other action as required.

6.3 Right to Request Amendment
Patients have the right to request in writing that PHI in a Covered Component’s Designated Record Set be amended. Note the patient does not have an unqualified right to amend, but has a right to request, and the Covered Component must consider the request as described below.

Procedure for Individual to Request Amendment
An individual who desires an amendment must provide the Covered Component a written statement identifying the portions of the record s/he considers inaccurate or incomplete, and the substitute or additional information s/he wishes to be added to the record. The individual may use BU’s approved form (see http://www.bu.edu/hipaa/forms-for-health-care-providers/) or may provide a substantially similar written request.

Covered Component’s Response to Request
Upon receiving a Request to Amend, the Covered Component’s HIPAA Contact shall review it. If the request is to correct demographic information or any information that originally came from the individual and which the individual says was recorded inaccurately, the HIPAA Contact, in his/her judgment, may make the correction. Examples include correcting spellings, ethnicity, date of birth and similar matters.

Any requests to amend information entered in the record by a treating health care provider (e.g., diagnosis; prognosis; history of condition; etc.) shall be forwarded to that provider and to the BU HIPAA Privacy Officer. The treating healthcare provider who made the entry will determine whether to allow the amendment. The request to amend may be denied if the original record is accurate.

The decision to grant or deny a request to amend should be made within 60 days of the request. If after 30 days the Covered Component has not been able to make a decision, it should contact the BU HIPAA Privacy Officer.
When the Covered Component Grants the Request to Amend

Within 60 days of receipt of the written request to amend, the Covered Component shall notify the individual that it has accepted the request, and shall make the change requested to the medical record, as follows:

Paper Record: Amendments will be made by drawing a single line through the original entry in such a way that the original entry remains legible. Where the entry has been changed the word “amendment” should be clearly printed at the incorrect entry, the correct information shall be entered, and the Covered Component staff person making the change should initial and date the correction.

Electronic Record: The Covered Component may make electronic corrections in such a way as to make it clear that an entry is being corrected, noting the person making the correction and the date of correction.

In addition to notifying the individual and making the change, the Covered Component should determine whether the information subject to the amendment has been disclosed to anyone outside of the Covered Component who may have had reason to rely on the amended information, and if so, shall forward the amended entry to those recipients.

When the Covered Component Denies the Request to Amend

Before denying a request to amend, the Covered Component must consult with the BU HIPAA Privacy Officer. The request to amend may be denied when the information to be amended:

- is not part of The Covered Component’s Designated Record Set;
- is accurate and/or complete; or
- was not created by The Covered Component (unless the individual can provide reasonable evidence that the originator of the PHI is no longer available to act on the amendment request, in which case, the Covered Component may include the individual’s statement of Amendment in its record).

The Covered Component must notify the individual of its decision, in plain language, including the following:

- the reason for denial;
- the individual’s right to submit a statement disagreeing with the denial and how the individual may file such statement;
- the individual’s right to ask that the original amendment request and denial be attached to any future disclosures of the information; and
- how to file a complaint with the Covered Component and/or the Secretary of Health and Human Services about the denial.

Recordkeeping

The completed Request for Amendment in Medical Record Form, the Covered Component’s Response and any statement of disagreement will be filed in the individual’s record.
6.4 Right to an Accounting of Disclosures

Patients have the right under HIPAA to request an Accounting of disclosures of their health information, and Covered Components have the obligation to fulfill such requests by following the procedures in this Policy.

Covered Components should contact the HIPAA Privacy Officer if any Request for Accounting is received.

What is in an Accounting?

The Accounting includes disclosures made without the individual’s Authorization within the 6-year period prior to the date of the request, or such shorter period as the Individual may request.

Example of disclosures included in an Accounting:

- Disclosures made for public health reporting;
- Disclosures made to government entities or law enforcement; and
- Disclosure for Research purposes;
  - If the research involves 50 or more individuals, the Accounting may provide only the following information:
    - Name of the research protocol;
    - Description of research activity;
    - Type of PHI disclosed;
    - Period of time during which disclosure was made; and
    - Contact information for the research sponsor and the researcher who received the information.

The following are excluded from an Accounting:

- Disclosures for treatment, payment or health care operations;
- Disclosures made to the individual (or authorized personal representative of the individual) who is the subject of the PHI;
- Disclosures made pursuant to a valid Authorization.
- “Incidental” disclosures, i.e., an unintended disclosure during the course of a permitted use or disclosure;
- Disclosures made to family members and friends involved in the individual’s care.
- Disclosures made for national security or intelligence purposes;
- Disclosures to correctional institutions, or custodial law enforcement officials;
- Disclosures made more than 6 years before the request for Accounting; and
- Disclosures made as part of a Limited Data Set in accordance with a Data Use Agreement when used solely to disclose a subset of information for research, public health or health care operations.

How the Individual Makes a Request for an Accounting

Requests for an Accounting of disclosures of PHI must be made in writing to the Covered Component. The Individual may use the “Request for an Accounting of Disclosures” form or may provide substantially the same information in another writing. The Covered Component should consult with the BU HIPAA Privacy Officer on any request for Accounting.
Time to Respond
The Covered Component must respond by providing the Individual an Accounting in writing within 60 days of the request. If after 30 days, it appears the Accounting may take longer, the BU HIPAA Privacy Officer may notify the individual in writing of the reason for the delay, and/or may extend time to provide the Accounting of disclosure by additional 30 days.

Information about Each Disclosure in Accounting
The following elements must be included for each disclosure listed on the Accounting of Disclosure:

1. Date of disclosure;
2. Receiving party, and address, if known;
3. Description of PHI disclosed;
4. A brief statement of the purpose of the disclosure;
5. If multiple disclosures were made to the same entity for the same purpose, the Covered Component must identify the number of times the disclosure was made and the date of the last such disclosure; and
6. Disclosures made by the Covered Component’ Business Associates, if made for purposes other than treatment, payment or health care operations (e.g., if a Business Associate responded to a subpoena for PHI of the Individual).

Accounting for disclosures made for research involving 50 or more individuals
When disclosures are made for research involving 50 or more individuals, the Accounting of Disclosures may be limited to providing to the individual the following information:

- The name of the research protocol or other research activity;
- A description of protocol or activity including purpose of research and criteria for selecting particular records;
- A brief description of the type of PHI that was disclosed;
- The date or time period during which disclosures occurred including date of last such disclosure;
- Information about the entity that sponsored the research and about the researcher to whom the information was disclosed; and
- A statement that the PHI may or may not have been disclosed for a particular protocol or other research activity.

Tracking Disclosures for Accounting Purposes
In order to be prepared to fulfill a request for Accounting, the Covered Component must track all disclosures of an individual’s PHI in the Designated Record Set that may be required in an Accounting.

Charge for Providing an Accounting of Disclosures
The Covered Component may not charge an individual requesting an Accounting of Disclosures for the first Accounting in a 12-month period. The Covered Component may charge a reasonable fee for subsequent requests in the same 12-month period.

Each Covered Component shall document its procedure on fees for an Accounting.
Denial Due to Special Circumstances
The Covered Component must temporarily suspend an individual’s right to receive an Accounting of disclosures to a health oversight agency or law enforcement official if such agency or official provides the Covered Component with a written statement that providing such an Accounting to the individual would impede the agency’s or official’s activities and specifying the time for which such suspension is required.

If the agency or official makes such a request orally, the Covered Component must document the statement including the name of the agency and official making the statement and must temporarily suspend the individual’s right to an Accounting of any disclosures made to such agency in accordance with the statement. Temporary suspensions may be allowed for a period not to exceed thirty (30) days from the date of an oral request; if the agency or official submits a written request for a suspension for a period longer than 30 days, the Covered Component shall comply.

6.5 Right to Request Restriction

Types of Restrictions Available
Patients have the right to request a restriction on uses and disclosure of their PHI. Typical requests include asking the Covered Component to not share any information, or a certain type of information, with a family member or friend of the Individual, which should be granted in most circumstances. The Covered Component should endeavor to accommodate all reasonable requests but should not agree to a restriction if it is not feasible to comply with it.

All requests for restriction shall be forwarded to the Covered Component’s HIPAA Contact, who must consult the BU HIPAA Privacy Officer before denying. The Covered Component should inform the Individual in writing of its decision.

An Individual may make a request for a restriction either in writing or orally. If an oral request is made, the Covered Component should document the request in the medical record. A form is available for requesting the restriction, but its use is optional. The Individual does not need to explain the reason for the request.

HIPAA recognizes that Individuals may wish to obtain specific health care services without informing their health care insurers. To that end, the following restriction must be accepted and implemented by the Covered Component:

- A request that the Covered Component not send specific information to the Individual’s health care insurer, if the Individual has paid for the service in full without recourse to that insurance.

The following uses and disclosures may not be restricted:

- All information must be available to provide treatment to the individual for emergency treatment purposes; if the Covered Component provides restricted information to another healthcare provider for emergency treatment purposes, the Covered Component shall request that the health care provider not further disclose the information;
- Uses and disclosures for which an Authorization or opportunity to agree or object is not required; such as in the cases of national security, public health activities, law enforcement, victims of abuse, neglect or domestic violence and research (see Policy 4 Non-Routine Uses and
Disclosures of PHI without Authorization, Section 4.1: Non-Routine Disclosures of PHI Permitted or Required by Law without Patient Authorization; and
• Disclosures required by the Secretary of the Department of Health and Human Services to investigate or determine compliance with HIPAA.

Terminating a Restriction
The Covered Component may terminate a restriction in the following circumstances:

• If the Individual requests and agrees to the termination in writing;
• If the Individual agrees to the termination orally and the oral agreement is documented; or
• If the Covered Component informs the Individual that it is terminating its agreement to a restriction, except that such termination is only effective with respect to PHI created or received after the Covered Component notifies the Individual of the termination.

The Covered Component may not terminate a restriction on disclosing information to the individual’s insurance company when the individual has paid for the services in full.

6.6 Right to Request Confidential and Alternate Modes of Communications
Individuals have the right to request that Covered Components communicate with them by an alternative means (e.g., written, electronic or oral) or at an alternative location (e.g., work, school or home). Requests should be submitted by the Individual in writing. A form is available for this purpose. The Individual is not required to provide a reason for the request.

Examples of alternate communication requests:

• Patient receives all dental care at GSDM Dental Center and bills are routinely sent to his home.
• Patient requests cosmetic services and requests that communications and billing on those services be sent to a PO Box.

Non-Secure Email/Text Requests
The Covered Component Workforce must use only the secure email system when communicating electronically with patients, and may not initiate, suggest or recommend non-secure email or text communications involving PHI.

However, if a patient requests communication via non-secure email or text message, the Covered Component shall do the following:

• Ensure the patient understands there is an option for secure email communication;
• If the patient still requests non-secure email or text message communication, the Covered Component must document the request by having the patient sign a Request for Non-Secure Email/Text Communication form or otherwise documentation his/her understanding that non-secure email or text may be intercepted. An email from the patient stating this is acceptable.

If a Workforce member receives a non-secure email or text from a patient, s/he should respond by sending a new message (DO NOT REPLY to avoid re-publishing any identifiable health information sent by the patient in the initial message):

Thank you for contacting me. [Covered Component] has a policy of not communicating with patients via regular email or text because they are not considered secure, and communications
may be intercepted. We use DataMotion, an encrypted email program, to communicate securely. Please reply to tell me your preference:

- to continue this correspondence via DataMotion or
- to continue using non-secure email or text despite the possibility of interception.

Accepting/Denying Other Requests
The Covered Component must consider any request to receive communications by an alternative means and make reasonable attempts to accommodate the request. However, the Covered Component should not agree to any request it cannot reasonably implement. Before denying any such request, the Covered Component’s HIPAA Contact must consult with the BU HIPAA Privacy Officer.

Upon acceptance/denial of such a request, the Covered Component will inform the Individual of its decision. If any Business Associate of the Covered Component may communicate with the Individual requesting a restriction, the Covered Component must inform that Business Associate.

6.7 Right to Complain
Covered Components must provide a process for their patients to make complaints if they believe their information privacy or security rights have been violated. The Covered Component may not retaliate against any patient who makes such a complaint.

BU EthicsPoint
Anyone, including patients, staff and others, wishing to make a confidential report about a possible privacy breach may do so at BU’s confidential hotline, EthicsPoint. Alternatively, a report may be made by telephone at 866-294-8451.

Resolution of Complaint
The BU HIPAA Privacy Officer and HIPAA Contact will endeavor to satisfy the patient’s concerns. If the BU HIPAA Privacy Officer finds no violation, s/he will notify the Individual in writing.

If the BU HIPAA Privacy Officer finds merit in the complaint after consultation with the Covered Component HIPAA Contact, s/he will notify the Individual of the findings and a proposed resolution to address harm, if any, to the Complainant. If investigation of the Complaint indicates a Workforce member has violated or contributed to a violation of these policies or of the law, disciplinary action will occur under Policy 7 Breaches, Section 7.5: Enforcement and Sanctions).
7. Breaches

7.1 Obligation to Report Potential Breaches
Any Workforce Member who learns that a potential breach of PHI may have occurred, s/he must immediately notify his or her supervisor and/or the Covered Component’s HIPAA Contact. The HIPAA Contact shall ensure the report is forwarded immediately to the BU HIPAA Privacy Officer. Reports may be sent to:

- the BU HIPAA Privacy Officer at hipaa@bu.edu
- BU Information Security Incident Response Team at irt@bu.edu or 617-358-1100

Failure to make a report in circumstances where the Workforce Member is required to do so may lead to discipline, up to and including termination of employment.

7.2 No Retaliation
Neither Covered Components nor anyone else affiliated with BU may intimidate, threaten, coerce, discriminate against, or take other retaliatory action against any individual for his/her exercise of any right established by, or for participation in any process provided for, these policies or the law, including:

- Filing a complaint with the Covered Component;
- Filing a complaint with governmental authorities;
- Assisting or participating in an investigation or compliance review by BU or its agents;
- Testifying in a proceeding or hearing by governmental authorities under HIPAA; or
- Opposing any act or practice made unlawful by HIPAA, provided the individual has a good faith belief that the practice opposed is unlawful and the manner of opposition is reasonable and does not involve an impermissible disclosure of PHI.

Individuals who report breaches may be subject to the protections of the University’s Code of Ethical Conduct.

7.3 Investigation and Remedial Action for Reports of Potential Breaches:

Responsibility to Receive, Record and Investigate Reports
BU’s HIPAA Privacy Officer and HIPAA Security Officer will:

- receive and respond to all notifications of the use or disclosure of PHI in violation of these Policies or of HIPAA;
- record all reports of potential breaches;
- investigate each according to the University’s Data Breach Management Plan to determine whether the circumstance constitute a breach; and
- document the conclusion.

In investigating electronic incidents the HIPAA Security Officer or HIPAA Contact follow Information Security’s First Responder Checklist to ensure that critical evidence is preserved. In addition, any
Workforce member should take reasonable precautions against physical threats to information, such as closing a door found open, locking cabinets and doors and similar steps.

**Confidentiality**

Upon request, BU will make all reasonable efforts to protect the confidentiality of persons reporting violations of law or of BU HIPAA policies or procedures to the extent practicable, given the nature of the investigation.

**Response to Breach**

If PHI has been used or disclosed in violation of BU policy or HIPAA requirements, BU will mitigate, to the extent practicable, any known harmful effects. Examples of actions that will be taken, depending on the circumstances, include the following:

- If the violation involves a continuing unauthorized disclosure of PHI, steps will be taken to end the practice immediately.
- If the violation involves an unlawful activity or practice, the activity or practice will be stopped, and the Office of the General Counsel will be notified of the violation.
- If the same or a similar violation could or might be prevented in the future by making changes to HIPAA policies and procedures, training or guidance, such changes will be instituted and promptly communicated to all affected employees.

**7.4 Breach Notifications**

In the event the BU HIPAA Privacy and/or Security Officer determines a Breach has occurred, they will notify the affected patients, the media and the Secretary, as applicable and as required under HIPAA, and will take appropriate remedial actions.

**7.5 Enforcement and Sanctions**

Members of the Workforce who are determined to have violated these policies or a Covered Component’s procedures may be subject to disciplinary action, up to and including termination of employment.
8. HIPAA Security Program

Philosophy

Boston University's HIPAA security program integrates the HIPAA Security Rule requirements into the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The CSF identifies the key, ongoing steps as: Identify, Protect, Detect, Respond, and Recover. This section is organized according to these five phases:

Responsibility for the security of patient information is shared between the HIPAA Components, BU IS&T and other BU central services. The sections below delineate the responsibility of each in specific areas. The BU HIPAA Privacy and Security Officers support the HIPAA Contacts in carrying out their responsibilities.

These polices are supplemented by Covered Component procedures based on the unique risks and needs of the individual Covered Components.

BU has other University-wide policies that impact information security, including but not limited to the Information Security Policy and the Data Protection Standards. These are not repeated in this Manual, but certain policies are referenced and linked in this document.

Defined Terms

**Device**: any electronic item that stores and processes (does something to or with) electronic data. This broad term includes desktop computers, laptops, tablets, mobile phones, medical devices, printers and fax machines that contain hard drives, and anything else that can store and process electronic data. Devices may be owned by BU or may be personal devices owned by the workforce member.

**Media**: any item that can store but not process data, including USB drives, CD-ROMs, DVDs, hard drives, back up disks.
**Application** is a computer program that processes information. Examples are Microsoft Outlook; electronic medical record programs; and programs that allow the sending and receiving of electronic data.

**System** means one or more computer servers and their related applications. For example, an electronic record system is composed of the servers, the electronic medical record application, the backup function and related applications.

**Data Center** is a physical location where servers are kept.

### 8.1 Identify

PHI can be protected only when we understand what it is, where it is, and who is authorized to access and use it. To that end, each Covered Component is responsible for identifying their PHI, where it is allowed to be stored, the members of their workforces, roles of their workforce members, and a process for providing, modifying and removing individual access to PHI.

#### 8.1.1 PHI Inventory

BU IS&T (and GSDM IT for the Dental Health Centers) inventory and track all BU devices (except for iPads, phones, medical devices, and fax machines) through its KACE system, and ensures those devices meet BU device standards for devices that access BU Restricted Use Data.

Covered Components document in their procedures:

- where PHI may be stored;
- whether its Workforce members are permitted to use personally-owned devices to access and store PHI;
- whether and how its Workforce members are permitted to access any systems containing PHI remotely;
- whether removable media such as CD-ROMs, DVDs and thumb drives may be used to store PHI and if so, how such media will be inventoried and tracked and what security measures must be followed.

The Covered Component PHI Inventory lists all personal devices and BU iPads, BU phones, BU medical devices, and fax machines permitted to store PHI. The inventories are maintained on the BU HIPAA SharePoint site. The inventory includes:

- Name for the asset (e.g., application, device, or server host)
- Description or identifier for each asset, such as a serial number, hardware specification or an application name
- Owner
- Administrators, if any
- Classifications, such as the device type
- Normal location

#### 8.1.2 Security Risk Assessments

The HIPAA Security Officer, working with the HIPAA Contacts, Information Security, and Internal Audit & Advisory Services and, from time to time as needed, external consultants, is responsible for conducting a comprehensive Security Risk Assessment that meets the requirements of the HIPAA Security Rule. The
assessment will, inter alia, document and prioritize all reasonably anticipated, high-level administrative, physical, and technical risks to the confidentiality, integrity, and availability of PHI.

The Security Risk Assessment confirms where PHI is located and identifies threats, vulnerabilities, risks, and controls, including an assessment of:

- threats to and vulnerabilities of those systems
- existing controls and countermeasures that mitigate those threats and vulnerabilities
- likelihood the vulnerabilities will be exploited by a threat
- potential impact of such threats and vulnerabilities on the confidentiality, integrity, and availability of PHI

These four factors (i.e., threats, vulnerabilities, likelihoods, and impacts to PHI) are combined to create an overall rating for each risk and identify areas where security controls are lacking. After completing the assessment, the HIPAA Security Officer and HIPAA Contacts meet to review the findings and create a Corrective Action Plan to address each identified risk. A summary of such assessments shall be made available to the Common Services and Information Security Governance Committee and others, as deemed appropriate.

The HIPAA Security Officer will perform or oversee a comprehensive risk assessment every 3-5 years. In the interim, the HIPAA Security Officer and Covered Component HIPAA Contacts shall review it at least annually and update it as needed on an ongoing basis, as described in the next section.

8.1.3 Periodic Technical and Non-Technical Security Reviews

The HIPAA Security Officer shall conduct periodic technical and non-technical reviews of the security of PHI to assess whether existing physical, technical, and administrative controls meet the requirements of this Policy and the Covered Components’ procedures. Reviews may involve inspecting system configurations, conducting vulnerability scanning or penetration testing, auditing documentation, checking physical controls such as doors and locks, looking at how devices are physically secured, verifying alarm and video systems are functioning, and other controls. These reviews may include an examination of security practices of Business Associates.

Security review findings shall be documented in the BU HIPAA SharePoint site and may require a Covered Component response.

HIPAA Contacts must notify the HIPAA Security Officer of any changes in the environment, operational procedure, or significant changes in the risks to PHI so that the Security Officer may perform an updated review. Often these involve new systems, applications or other changes that may affect the security of PHI. These reviews may have a smaller scope, such as the planned acquisition of a new software package or physical relocation.

8.2 Protect

8.2.1 Individual Responsibilities

See Section 2 of this HIPAA Policy Manual.
8.2.2 Administrative Controls: Training, Access Management

Training: See Section 1.8: HIPAA Training.

Security training is part of annual HIPAA training. In addition, the HIPAA Security Officer will periodically issue reminders and updates about security issues of critical concern. Covered Components will ensure these reminders reach all members of the Covered Component Workforce.

Access Management: Covered Components create and document procedures that define how access to PHI is authorized, maintained, and revoked, including a matrix of access rights based on Workforce member roles, following the Minimum Necessary standard (see Policy 3.2).

The Dental Health Centers maintain their documentation of changes to access rights (provision, alteration, or removal) on the GSDM “portal.” The other Covered Components maintain this documentation on the BU HIPAA SharePoint site.

Access to PHI is terminated immediately when such access is no longer required due to a workforce member leaving a role, unless an Exception is granted pursuant to Section 10.0.

8.2.3 Technical Controls

Technical controls are software and logical controls to prevent unauthorized activity that may pose a threat to the confidentiality, integrity or availability of PHI. Following are technical controls common to all:

- Accounts with access to PHI require strong passwords as specified in the University’s Data Protection Standards for Identity and Access Management.
- Access to PHI requires two-factor authentication wherever possible. When two-factor authentication is not possible, quarterly password changes is an acceptable alternative.
- Each individual accessing a system or application is identified uniquely and account credentials may not be shared, unless approved by an Exception pursuant to Policy 10.
- Systems and applications require authentication when left idle. Maximum idle time for PHI systems or applications is 15 minutes. Alternatively, the device idle time may be set to 15 minutes, without signing out of a particular application.
- Administrative rights to systems and applications are granted only where required for job function.
- Removable media have been blocked from all BU devices in the Covered Components using Microsoft Group Policy, except for those devices or whitelisted removable media that the Security Officer and HIPAA Contact agree are necessary. Those devices or whitelisted removable media are listed in the CC procedures inventory.

Additional technical controls specific to each Covered Component are documented in their HIPAA procedures.

8.2.3.1 Encryption

Data Centers: PHI within data centers is encrypted at-rest, except where the HIPAA Privacy and Security Officers have granted an exception pursuant to Policy 10 of the HIPAA Policy Manual.

Devices: All devices (e.g., desktop computers, laptops, phones, USB thumb drives, CDs, backup tapes) used to access or store PHI must use encryption at rest to protect the data if the device is lost or stolen.
Any devices, either personal or University owned, that access or store PHI and do not use encryption at rest must be documented as an Exception pursuant to HIPAA Policy 10.

Transmission: All PHI must be encrypted in transit and must use integrity controls except where the HIPAA Privacy and Security Officers have granted an exception pursuant to Policy 10 of the HIPAA Policy Manual.

8.2.3.2 Anti-malware Software Protection
All systems that store or access PHI must run anti-malware software approved by the HIPAA Security Officer for detecting and preventing the execution of malicious software.

BU IS&T will install anti-malware on all BU systems, devices and applications that access PHI. Covered Components are responsible for ensuring permitted personal devices have anti-malware. BU IS&T offers anti-malware at no cost for both BU and personal devices.

Anti-malware must run at all times and must be set to automatically update and scan.

8.2.3.3. Backups
All systems and applications that store PHI must be securely backed up. Covered Components describe the backup mechanism or procedure for each in the Covered Component Inventory.

8.2.3.4. System and Application Auditing
BU IS&T is responsible for auditing systems and applications run by BU IS&T centrally, such as RU-GPNAS network drives. Covered Components document auditing procedures for applications unique to each, such as Component electronic medical records.

8.2.4 Physical Controls
8.2.4.1. Covered Component Facility Physical Security Plan
Each Covered Component has a floor plan maintained by Boston University Real Estate and Facility Services that documents the physical structures, such as rooms and locking doors that protect PHI from theft and other physical threats. The Security Officer reviews these floor plans with each Covered Component and works with Boston University Real Estate and Facility Services to correctly document the physical structures. Plans approved by the Security Officer are stored on the HIPAA SharePoint site.

The Dental Health Centers maintain an inventory of keys (presently in CAMMS, BU Facilities Service Request system), where each key must be linked to a UID. Each department is responsible for deciding and tracking who gets keys, and reporting when any individual or shared key is lost. The other Covered Components maintain an inventory of physical keys on the BU HIPAA SharePoint site.

BUPD on the Charles River Campus and BU Public Safety on the Medical Campus provide security monitoring and response.

Boston University ID Card provides a method for positively identifying members of a Covered Component Workforce (UID). Vendors and guests in areas that provide access to PHI must either be escorted or have visitor badges.

The HIPAA Contact is responsible for ensuring that repairs and modifications to their physical components are managed in such a way as to maintain the security of PHI, are correctly documented in
the Covered Component floor plan, and for contacting the HIPAA Security Officer for assistance as needed.

8.2.4.2. Data Center Physical Security
BU IS&T is responsible for the security of all BU IS&T data centers, including access control.

Any Covered Component that wishes to establish a new data center must consult the Security Officer and comply with all BU information security policies.

8.2.4.3. Security in Business Processes
This HIPAA Contact is responsible for ensuring that reasonable precautions are taken to prevent unauthorized access to PHI during the course of normal, daily operations consistent with the BU Individual Responsibilities policy at Section 4.0 of this HIPAA Policy Manual. For example, devices used for accessing PHI should not be accessible to the public, monitors displaying PHI should be pointed away from public areas, servers must be kept in locked data centers with appropriate environmental controls, and portable devices must not be stored in areas where they can be easily stolen. In addition, business processes must be designed to ensure data is kept secure.

8.2.4.4. Device and Media Security
Devices outside of a data center that have a documented Exception to store unencrypted PHI, and that are not intended to be mobile, must be physically secured using locking pads, cables, or similar technologies, unless stored in a significantly secured physical space. Permitted personal devices must meet the same security standards as BU owned devices, which means the device is:

- Entered onto the Covered Component PHI inventory
- Has been checked by BU IT to confirm it has:
  - encryption turned on,
  - has anti-malware installed,
  - has an idle time of 15 minutes or less, and
  - has an operating system that is supported and regularly updated.

BU IS&T provides secure destruction of physical devices and media pursuant to the University’s Data Protection Requirements and Media Destruction One-Sheets. This service is available free of charge.

Any device or media containing PHI that has reached the end of its useful life must be delivered to IS&T for secure destruction even if the PHI was encrypted.

IS&T and GSDM IT record destruction of KACE-controlled devices; Covered Components record destruction of other devices and media on their Inventories.

8.3 Detect: Information System Activity Reviews
BU IS&T monitors central systems such as the Campus Edge Firewall and notifies the HIPAA Privacy Officer and/or HIPAA Security Officer of events of any concern that may involve PHI for their further investigation.
IS&T and GSDM IT reviews are documented in ServiceNow (BU’s IT service tracking system) in accordance with a Knowledge Base Article that is maintained by the HIPAA Security Officer.

The Covered Components are responsible for System Activity Reviews of any systems, devices and applications unique to them, for example, their electronic medical records or any medical devices. The plan for such review will be created jointly by the HIPAA Contact and HIPAA Security Officer, based on an assessment of the risks posed by the operations and nature of activities of the Covered Component, aimed at detecting e.g., unauthorized access, unusual uses, or suspicious disclosures. These will be documented in the Covered Component’s HIPAA Procedures.

Covered Component reviews are documented on the HIPAA SharePoint site.

8.4 Respond

A security incident is an “attempted or successful unauthorized access, use, disclosure, modification, or destruction of information or interference with system operations in an information system” (45 C.F.R. § 164.304). Typically, only successful unauthorized access, use, disclosure, modification or destruction will constitute a breach under HIPAA, as determined by the HIPAA Privacy and Security Officers.

Any Workforce Member who suspects a security incident may have occurred must immediately notify his or her HIPAA Contact and the BU Information Security Incident Response Team at irt@bu.edu or 617-358-1100. Incidents may also be reported to hipaa@bu.edu or anonymously to the BU EthicsPoint.

For more information, see Section 7: Breaches.

8.5 Recover: Contingency Planning; Emergency Mode Operations; Recovery

BU’s Emergency Management Department is responsible for Covered Components’ Emergency Management Plans. Each takes into account how PHI will be protected during an unforeseen event such as a power outage caused by a utility failure, or a natural disaster such as fire, flood, or earthquake. The plans include evacuation plans with an emphasis on how patients are cared for when in the middle of a session or procedure when an evacuation is required.

BU IS&T is responsible for responding to electronic emergencies, such as a cybersecurity attack to gain access to PHI or to deny service, or a network outage.

Covered Components supplement the emergency management services provided by the University with Continuity of Operations Plan (COOP) specific to their healthcare practices, including, for example:

- Workforce responsibilities in responding to an event
- Emergency communication plans, including provider and staff phone lists and rally points
- Dissemination of emergency management plans.
The healthcare services provided by BU’s Covered Components are all outpatient services of an elective nature and therefore there is no plan to continue to provide services during an emergency. In all emergencies and disasters, the Covered Component Workforce will follow their BU Emergency Response and Recovery plans under the direction of the Emergency Management Department and BU Police or Public Safety, to protect the safety of Workforce members and patients and physical assets, including those holding PHI.

Planned responses to specific emergency situations are described below.

- **Unavailability of EMR:** In the event the Covered Component’s EMR is unavailable for more than a brief time, providers will record information physically using pen and paper, or electronically using available electronic resources (such as Microsoft Word). Any physical records created will be secured in accordance with the standards provided in Section 2.0 of the HIPAA Policy Manual. Any electronic PHI created outside the medical record must be stored in a location approved for PHI and Restricted Use Data, such as Microsoft OneDrive or an approved network drive. Upon the reactivation of the EMR, the HIPAA Contact and clinical leaders of each affected component will meet to determine how the physical PHI will be added to the EMR to ensure the completeness and integrity (for example, following a brief interruption, providers may be responsible for entering all data themselves and destroying securely all physical PHI that has been electronically entered). If the duration of the interruption is long enough that this will be inefficient, the HIPAA Contact and clinical leaders will determine whether other members of the Covered Component workforce will assist; whether assistance will be provided by BU resources outside of the Covered Component, or whether external resources will be used. The usual rules apply. BU resources outside the Covered Component will be treated as Support Units and subject to the same obligations as Support Units. External resources will be required to execute a Business Associate Agreement before accessing PHI.

- **Unplanned Destruction of Electronic Medical Records:** Covered Components other than the Dental Health Centers use a third-party provider electronic medical record. Each of those third parties is responsible for backing up the data in the electronic medical record and will be key participants in restoring access and confirming the integrity of the data. The HIPAA Contact is responsible for coordinating this effort. GSDM IT is responsible for back up and restoration of Salud and Eaglesoft.

- **Unplanned Destruction of BU Drives, Systems:** IS&T is responsible for back up and restoration of any BU central systems and applications.

- **Severe and Disabling Emergency:** In the event of a severe emergency that renders a Covered Component incapable of providing any health services to its patients, patients will be directed to the nearest emergency facility for urgent medical needs. This will be done through a sign posted at the patient entrance of each such facility, by recorded message at the main telephone number used by patients, and online, as coordinated with BU Emergency Management Department. The HIPAA Contact is responsible for ensuring this is done. Following that step, the HIPAA Contact and clinical leadership of the component will meet to determine other appropriate steps that may include individual providers using reasonable efforts to contact patients deemed to be in immediate need of care to assist them in making alternate care arrangements.
• **When Physical Space is Unavailable:** Physical space regularly used by Covered Components to provide health services may be rendered unusable for an extended period of time by fire, flood, earthquake, terrorist attack and other natural and man-made disasters. If this occurs, BU Emergency Management Department and Facilities Management will head the effort to secure an alternate location. The HIPAA Contact, with the support of the BU HIPAA Privacy and Security Officers, will ensure such alternate locations meet BU’s HIPAA standards and/or for approving temporary Exceptions pursuant to Section 10.0 of this HIPAA Policy Manual.
9. Documentation and Retention

The University must keep documentation of:

- Current security policies and procedures implemented by the Component, and
- An archive of policies that were valid anytime in the past six calendar years.

The HIPAA Privacy Officer and HIPAA Security Officer shall maintain the archive of all University level policies. The HIPAA Contact must maintain this documentation of any procedure created or maintained by the Covered Component.

In addition, many portions of the security program require documentation of activity, most notably granting and reviewing access, and reviewing information system activity. The Covered Components must keep documentation of all such actions for a period of six years.
10. Exceptions

The HIPAA Privacy Officer and HIPAA Security Officer will jointly review any requested exceptions to the requirements set forth in this Policy. Exceptions will be granted if a thorough review of the situation demonstrates appropriate compensating controls have been implemented, and the risk posed by the exception is reasonable and acceptable.

If the requested exception also involves a deviation from standards and policies of the BU IS&T department, the Covered Component must contact IS&T for a separate waiver or exception of those policies.
11. Definitions

Application is a computer program that processes information. Examples are Microsoft Outlook 365; electronic medical record programs; and programs that allow the sending and receiving of electronic data.

Data Center is a physical location where servers are kept.

Device means any electronic item that stores and processes (does something to or with) electronic data. This broad term includes desktop computers, laptops, tablets, mobile phones, medical devices, printers and fax machines that contain hard drives, and anything else that can store and process electronic data. Devices may be owned by BU or may be personal devices owned by the workforce member.

Disclosure means the release, transfer, provision of access to, or divulging in any manner of information outside the entity holding the information.

Electronic media means: (1) Electronic storage material on which data is or may be recorded electronically, including, for example, devices in computers (hard drives) and any removable/transportable digital memory medium, such as magnetic tape or disk, optical disk, or digital memory card; (2) Transmission media used to exchange information already in electronic storage media. Transmission media include, for example, the Internet, extranet or intranet, leased lines, dial-up lines, private networks, and the physical movement of removable/transportable electronic storage media. Certain transmissions, including of paper, via facsimile, and of voice, via telephone, are not considered to be transmissions via electronic media if the information being exchanged did not exist in electronic form immediately before the transmission.

Electronic protected health information means information that comes within paragraphs (1)(i) or (1)(ii) of the definition of protected health information as specified in this section.

Health care means care, services, or supplies related to the health of an individual. Health care includes, but is not limited to, the following: (1) Preventive, diagnostic, therapeutic, rehabilitative, maintenance, or palliative care, and counseling, service, assessment, or procedure with respect to the physical or mental condition, or functional status, of an individual or that affects the structure or function of the body; and (2) Sale or dispensing of a drug, device, equipment, or other item in accordance with a prescription.

Health care component means a component or combination of components of a hybrid entity designated by the hybrid entity in accordance with § 164.105(a)(2)(iii)(D).

Health care operations means any of the following activities of the covered entity to the extent that the HIPAA Administrative Simplification Regulation Text March 2013 75 activities are related to covered functions:

(1) Conducting quality assessment and improvement activities, including outcomes evaluation and development of clinical guidelines, provided that the obtaining of generalizable knowledge is not the primary purpose of any studies resulting from such activities; patient safety activities (as defined in 42 CFR 3.20); population-based activities relating to improving health or reducing health care costs, protocol development, case management and care coordination, contacting of health care providers and patients with information about treatment alternatives; and related functions that do not include treatment;
(2) Reviewing the competence or qualifications of health care professionals, evaluating practitioner and provider performance, health plan performance, conducting training programs in which students, trainees, or practitioners in areas of health care learn under supervision to practice or improve their skills as health care providers, training of non-health care professionals, accreditation, certification, licensing, or credentialing activities;

(3) Except as prohibited under § 164.502(a)(5)(i), underwriting, enrollment, premium rating, and other activities related to the creation, renewal, or replacement of a contract of health insurance or health benefits, and ceding, securing, or placing a contract for reinsurance of risk relating to claims for health care (including stop-loss insurance and excess of loss insurance), provided that the requirements of § 164.514(g) are met, if applicable;

(4) Conducting or arranging for medical review, legal services, and auditing functions, including fraud and abuse detection and compliance programs;

(5) Business planning and development, such as conducting cost-management and planning related analyses related to managing and operating the entity, including formulary development and administration, development or improvement of methods of payment or coverage policies; and

(6) Business management and general administrative activities of the entity, including, but not limited to: (i) Management activities relating to implementation of and compliance with the requirements of this subchapter; (ii) Customer service, including the provision of data analyses for policy holders, plan sponsors, or other customers, provided that protected health information is not disclosed to such policy holder, plan sponsor, or customer. (iii) Resolution of internal grievances; (iv) The sale, transfer, merger, or consolidation of all or part of the covered entity with another covered entity, or an entity that following such activity will become a covered entity and due diligence related to such activity; and (v) Consistent with the applicable requirements of § 164.514, creating de-identified health information or a limited data set, and fundraising for the benefit of the covered entity.

Health care provider means a provider of services (as defined in section 1861(u) of the Act, 42 U.S.C. 1395x(u)), a provider of medical or health services (as defined in section 1861(s) of the Act, 42 U.S.C. 1395x(s)), and any other person or organization who furnishes, bills, or is paid for health care in the normal course of business.

Health information means any information, including genetic information, whether oral or recorded in any form or medium, that:

(1) Is created or received by a health care provider, health plan, public health authority, employer, life insurer, school or university, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual.

Hybrid entity means a single legal entity:
Individual means the person who is the subject of protected health information. Individually identifiable health information is information that is a subset of health information, including demographic information collected from an individual, and:

(1) Is created or received by a health care provider, health plan, employer, or health care clearinghouse; and

(2) Relates to the past, present, or future physical or mental health or condition of an individual; the provision of health care to an individual; or the past, present, or future payment for the provision of health care to an individual; and

   (i) That identifies the individual; or

   (ii) With respect to which there is a reasonable basis to believe the information can be used to identify the individual.

Media means any item that can store but not process data, including USB drives, CD-ROMs, DVDs, hard drives, back up disks.

Protected health information means individually identifiable health information:

(1) Except as provided in paragraph (2) of this definition, that is:

   (i) Transmitted by electronic media;

   (ii) Maintained in electronic media; or

   (iii) Transmitted or maintained in any other form or medium.

(2) Protected health information excludes individually identifiable health information:

   (i) In education records covered by the Family Educational Rights and Privacy Act, as amended, 20 U.S.C. 1232g;

   (ii) In records described at 20 U.S.C. 1232g(a)(4)(B)(iv);

   (iii) In employment records held by a covered entity in its role as employer; and

   (iv) Regarding a person who has been deceased for more than 50 years.

Research means a systematic investigation, including research development, testing, and evaluation, designed to develop or contribute to generalizable knowledge.

System means one or more computer servers and their related applications. For example, the GSDM electronic system is composed of the servers, the electronic medical record, the backup function and related applications.

Treatment means the provision, coordination, or management of health care and related services by one or more health care providers, including the coordination or management of health care by a health care provider with a third party; consultation between health care providers relating to a patient; or the referral of a patient for health care from one health care provider to another.
Use means, with respect to individually identifiable health information, the sharing, employment, application, utilization, examination, or analysis of such information within an entity that maintains such information.

Workforce means employees, volunteers, trainees, and other persons whose conduct, in the performance of work for a covered entity or business associate, is under the direct control of such covered entity or business associate, whether or not they are paid by the covered entity or business associate.
Effective April 10, 2017:
The BU HIPAA Privacy Officer is Diane Lindquist, 617-358-3124, dlindq@bu.edu
The BU HIPAA Security Officer is David Corbett, 617-414-1475, corbettd@bu.edu
General questions on HIPAA: hipaa@bu.edu
Report breaches: irt@bu.edu

The HIPAA Contacts designated by the Covered Components as of November 1, 2018 are as follows:

<table>
<thead>
<tr>
<th>Covered Component</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>GSDM Dental Health Centers</td>
<td>Mollie Forman</td>
</tr>
<tr>
<td>Danielsen Institute</td>
<td>Lauren Kehoe</td>
</tr>
<tr>
<td>Student Health Services</td>
<td>Judy Platt, MD</td>
</tr>
<tr>
<td>Sargent Choice Nutrition</td>
<td>Stacey Zawacki</td>
</tr>
<tr>
<td>BU Rehabilitation Services</td>
<td>James Camarinos</td>
</tr>
</tbody>
</table>

The HIPAA Contacts designated by the Support Units are as follows:

<table>
<thead>
<tr>
<th>Support Unit</th>
<th>Contact</th>
</tr>
</thead>
<tbody>
<tr>
<td>Information Services and Technology</td>
<td>Eric Jacobsen</td>
</tr>
<tr>
<td>Office of General Counsel</td>
<td>Lilly Huang</td>
</tr>
<tr>
<td>Compliance</td>
<td>Nedra Abbruzzese-Werling</td>
</tr>
<tr>
<td>Risk Management</td>
<td>James Donohue</td>
</tr>
<tr>
<td>Internal Audit and Advisory Services</td>
<td>Andrew James Soares</td>
</tr>
<tr>
<td>Finance</td>
<td>Matt Abrams</td>
</tr>
<tr>
<td>Human Resources</td>
<td>Diane Tucker</td>
</tr>
</tbody>
</table>